DATENSCHUTZBEWERTUNG VON STATE-OF-THE-ART LERNMANAGEMENT-SYSTEMEN

DIPLOMARBEIT

TECHNISCHE UNIVERSITÄT DRESDEN
FAKULTÄT INFORMATIK
DOZENTUR KOOPERATIVE MULTIMEDIALE ANWENDUNGEN

Vorgelegt von Anne-Katrin Stange
14. September 2007

Hochschullehrer: Doz. Dr. Hilko Donker
Betreuerin: Dipl. Inform. Katrin Borcea-Pfitzmann

Inhalt

1. Einleitung und Motivation…….. 7

2. Lernmanagement-Systeme…….. 9
   - 2.1 Begriffsdefinition……... 9
   - 2.2 Auswahl von State-of-the-Art Lernmanagement-Systemen…….. 12
   - 2.3 Abgrenzung des Untersuchungsgebietes……... 15
   - 2.4 Zusammenfassung……... 19

3. Gesetzliche Grundlagen zum Datenschutz und der Informationellen Selbstbestimmung…… 20
   - 3.1 Internationale Regelungen…….. 20
     - 3.1.1 Europarat…… 20
     - 3.1.2 OECD……. 21
     - 3.1.3 Europäische Gemeinschaft…… 21
   - 3.2 Nationale Datenschutzgesetze…… 24
   - 3.3 Vergleich nationaler und internationaler Gesetze……... 26
   - 3.4 Datenschutzgesetze in Bezug auf das eLearning…… 27
   - 3.5 Datenschutzgesetze in Bezug auf Minderjährige…… 28
   - 3.6 Zusammenfassung……... 29

4. Methodik der Datenschutzbewertung…….. 31
   - 4.1 Rezessionen……. 31
   - 4.2 Vergleichsgruppen……... 31
   - 4.3 Expertenurteil……... 32
   - 4.4 Kriterienkataloge……. 32
   - 4.5 Geplante Durchführung der Bewertung……... 33

5. Die Bewertungskriterien……... 35
   - 5.1 Recherche von Kriterien für eine Datenschutzbewertung……... 35
     - 5.1.1 Bewertungskriterien für Softwareprodukte…… 35
     - 5.1.2 Bewertungskriterien für eLearning-Systeme…….. 37
       - 5.1.2.1 Datenschutzkriterien im universitären Umfeld…….. 37

5.1.2.2 Sicherheits- und Datenschutzkriterien im eLearning……. 40
5.1.2.3 Sicherheit- und Datenschutzkriterien bei Lernmanagement-Systemen…….. 45
5.2 Kriterien für diese Evaluation…….. 46
5.2.1 Kriterium: Datensparsamkeit…….. 46
5.2.2 Kriterium: Zweckbestimmung und Nutzungsbegrenzung…….. 47
5.2.3 Kriterium: Rollen und Zugriffsrechte……. 47
5.2.4 Kriterium: Rechte des Betroffenen und Informationelle Selbstbestimmung……... 48
5.2.5 Kriterium: Sicherheit und Datenqualität……. 49
5.3 Zusammenfassung……... 50

6. Ergebnisse der Untersuchung……... 52
6.1 Allgemeine Beobachtungen……. 52
6.2 Auswertung anhand der einzelnen Lernmanagement-Systeme……... 54
6.2.1 Blackboard……... 54
6.2.2 CLIX…… 57
6.2.3 WebCT……. 59
6.2.4 ILIAS……... 63
6.2.5 Moodle……. 66
6.2.6 OLAT……... 69
6.2.7 BluES'n…… 72
6.2.8 Zusammenfassung……... 77
6.3 Auswertung anhand der einzelnen Bewertungskriterien……. 78
6.3.1 Datensparsamkeit……. 78
6.3.2 Zweckbestimmung und Nutzungsbegrenzung……. 78
6.3.3 Rollen und Zugriffsrechte…… 79
6.3.4 Rechte des Betroffenen und Informationelle……... 79
6.3.5 Sicherheit und Datenqualität…… 80
6.4 Vergleich zur Studie „Privacy in eLearning"…….. 81
7. Ausblick und Zusammenfassung……..…… 85

Abbildungsverzeichnis…… 87
Tabellenverzeichnis…… 88
Literatur und Quellenverzeichnis…… 89
Anhang…… 93

1.Einleitung und Motivation

In der klassischen universitären Lehre sowie im Schulwesen waren Datenschutzbestimmungen auf klar abzugrenzende Gebiete anzuwenden. Durch die vernetzten Informationstechniken, die uns heutzutage umgeben, kommen immer mehr Personen mit personenbezogenen Daten in Kontakt. So werden Informationen gesammelt und gespeichert, die entweder durch die Lernenden selbst erstellt wurden, oder durch deren Aktionen über sie generiert werden. Auch bei der Entwicklung von Software-Anwendungen, die Informationen von Lernenden verarbeiten und der Unterstützung universitärer Abläufe dienen, wird meist ohne Sicht auf gesetzliche Grundlagen des Datenschutzes die Verarbeitung von Informationen vorgenommen [CAU97]. Durch neue verteilte Architekturen ist es nicht nur möglich, Informationen von und über Lernende in strukturierten Datenbanken zu halten, sondern Daten können auch durch elektronische Transaktionen schnell und reibungslos ausgetauscht werden. Dadurch ist es heutzutage auch weniger schwierig, auf diese Daten zuzugreifen, sie zu manipulieren, oder weiterzutransportieren. Genauso ist bei einer Übertragung der Daten durch Netzwerke beziehungsweise das Internet nicht gewährleistet, dass der Empfänger der Nachricht der Einzige ist, der diese lesen kann. Eine ungesicherte Übertragung der Daten kann somit die Sicherheit und den Datenschutz beinträchtigen.
Universitäten und Dozenten verwenden vernetzte Technologien, um neue Möglichkeiten für das Lehren und Lernen zu fördern und um Serviceleistungen für Studenten zu verbessern. So ermöglichen die Informationstechnologien einerseits eine Unterstützung universitärer Prozesse, was den Datenschutz in einer neuen Form beeinträchtigt. Andererseits ermöglichen diese Techniken auch neue Vorgehensweisen, um personenbezogene Daten zu schützen.
Durch die immer weiter schreitenden technologischen Entwicklungen wurde schon 1997 von CAUSE [CAU97] eine Evaluation von Datenschutzrichtlinien hinsichtlich des entstehenden Ubiquitous Computing und der Netzwerktechnologien durchgeführt, um rechtzeitig mögliche Anpassungen vorzunehmen und auch in diesem Umfeld den Datenschutz zu gewähren. In ihrer Arbeit forderten die Autoren weitgreifende Anpassungen der bestehenden Datenschutzpraktiken.

Bei eLeaning-Systemen ist die Möglichkeit, zeit- und ortsunabhängig an virtuellen Kursen mittels unterschiedlichster IT-Geräte teilzunehmen, als ein großer Vorteil gegenüber klassischen Lehrmethoden zu sehen. eLearning umfasst dabei für diese Arbeit alle Lernanwendungen, die über das Internet erreichbar sind oder mittels des Internets ausgeführt werden. Durch die Technologien des eLearning kann außerdem die Anpassung der Lernmaterialien an die Anforderungen und Bedürfnisse der Benutzer vorgenommen werden. Dies kann aber auch mit einer verstärkten Überwachung der Lernaktivitäten des Lernenden einhergehen.
Bisher fokussierten viele Entwicklungen im eLearning primär die geeignete Umsetzung von Lernstoff sowie die Unterstützung des Lernweges. Eine Auseinandersetzung mit Fragen der Sicherheit und des Datenschutzes fand dabei wenig bis gar nicht statt. Nach dem bisherigen Fokus im eLearning gibt es aber auch einen Bedarf an Privatheit und Datenschutz in den e-Learning-Systemen, der durch geeignete Technologien und Maßnahmen erreicht werden kann. Dass es eine Nachfrage nach Privatheit und Datenschutz in eLearning-Systemen gibt, konnte ebenfalls in einer 2006 durchgeführten Umfrage nachgewiesen werden [Sta06]. Dort gaben etwa 75% der Teilnehmer an, besorgt um den Schutz ihrer Privatheit zu sein - bei der Verwendung von Internetangeboten genauso wie bei eLearning-Diensten. Insbesondere befürchteten sie, dass personenbezogene Daten für Zwecke verwendet werden, die nicht vom Benutzer bewilligt wurden.

Es soll Inhalt dieser Arbeit sein, die spezielle Form des eLearning, die mittels Lernmanagement-Systemen durchgeführt wird, auf deren Unterstützung von Datenschutzbestimmungen zu untersuchen und zu bewerten. Darüber hinaus soll ermittelt werden, ob die Systeme den Bedürfnissen von eLearning-Benutzern hinsichtlich des Schutzes ihrer Privatheit gerecht werden. Insbesondere ist es von Interesse, in welchem Maße der Datenschutz und der Schutz der Privatheit der Benutzer eines Lernmanagement-Systems in ausgewählten Lernplattformen integriert sind. Dies soll unter Berücksichtigung von Datenschutzkriterien durchgeführt werden. Ebenfalls soll ein bewertender Vergleich der Ergebnisse der Datenschutzbewertung mit den Resultaten der Studie „Privacy in eLearning“ erarbeitet werden.
Da der Begriff „Lernplattform“ häufig als Synonym für Lernmanagement-Systeme verwendet wird, sollen die Begriffe auch in dieser Arbeit gleichgesetzt werden.
Innerhalb dieser Arbeit werden die Begriffe persönliche, private, personenbezogene Daten und Informationen verwendet, mit denen zum Ausdruck gebracht wird, dass es sich um Daten über ein Individuum handelt, mit denen es identifizierbar ist oder dadurch die Möglichkeit besteht es zu identifizieren. Diese Begriffe werden synonym gebraucht. Des Weiteren wird der Begriff Aktivitätsdaten als weitere sensible Informationen verstanden, die von einem Lernmanagement-System gesammelt werden können. Dazu gehören Informationen, wie Datum, Dauer und Häufigkeit von Zugriffen eines Benutzers auf Funktionen und Objekte der Lernplattform.

In Kapitel 2 der Arbeit wird zunächst definiert, welche Eigenschaften ein Lernmanagement-System ausmachen. Daraufhin sollen geeignete Kandidaten für die Bewertung identifiziert werden. Darüber hinaus wird hier auch der Rahmen der Untersuchung festgelegt.
Im dritten Kapitel werden internationale und nationale Datenschutzgesetzgebungen betrachtet, die die Privatheit von Individuen schützen sollen. Dabei wird auf die jeweiligen Datenschutzprinzipen eingegangen, sowie auf die Auswirkungen und Einflüsse der Datenschutzgesetzgebungen. In Kapitel 4 werden verschiedene Methoden zur Evaluation von Softwaresystemen vorgestellt und deren Angemessenheit für die durchzuführende Untersuchung bewertet. Im fünften Kapitel werden nach einer Präsentation von Vorgehen bei Datenschutzbewertungen aus angrenzenden Gebieten die eigenen Bewertungskriterien für die Datenschutzbewertung vorgestellt.
Die Ergebnisse der Datenschutzbewertung werden im sechsten Kapitel vorgestellt und analysiert. Dabei wird zuerst auf allgemeine Beobachtungen, die während der Durchführung der Bewertung aufgetreten sind, eingegangen. Daraufhin werden die Lernmanagement-Systeme anhand der aufgestellten Kriterien bewertet. Eine Schlussfolgerung dieser Ergebnisse wird im weiteren Verlauf vorgenommen. In diesem Kapitel wird auch ein Vergleich zu den Resultaten der Studie [Sta06] vorgestellt, der zusammenfasst, ob und wie die Bedürfnisse von eLearning-Benutzern in Lernmanagement-Systemen erfüllt werden können. Kapitel 7 gibt einen Ausblick über die ermittelten Resultate.

2. Lernmanagement-Systeme

Dieses Kapitel beschäftigt sich im ersten Abschnitt mit der Begriffsbestimmung und Abgrenzung von Lernmanagement-Systemen gegenüber anderen eLearning-Systemen. Daraufhin wird im zweiten Abschnitt eine Auswahl der Lernmanagement-Systeme vorgenommen, die in der weiteren Arbeit untersucht werden sollen. Abschnitt 3 beinhaltet die Abgrenzung des Bereiches, der bei der Untersuchung betrachtet werden soll.

2.1 Begriffsdefinition

Durch Computer-Systeme und deren Vernetzung haben sich unter anderem auch die Möglichkeiten für das Lernen und Lehren erweitert. Nicht nur Hypertextsammlungen und Online-Präsentationen von Lehrskripten sind möglich sondern auch die Verlagerung des gesamten Lehr-Lern-Prozesses ins Internet. Lernmanagement-Systeme (engl. Learning Management Systems; abgekürzt LMS) stellen durch ihre Funktionalitäten eine mächtige Form des Online-Lernens zur Verfügung. Als ein wesentlicher Vorteil gegenüber der klassischen Lehre kann die Möglichkeit des orts- und zeitunabhängigen Lehrens und Lernens angesehen werden.

Die Ansichten unterschiedlicher Autoren darüber, was im Einzelnen unter einem Lernmanagement-System zu verstehen ist, werden nun vorgestellt. Es wird dabei analysiert, durch welche Merkmale ein Lernmanagement-System beschrieben und welcher Konsens daraus gebildet werden kann. Da die Untersuchung von Lernmanagement-Systemen hinsichtlich ihrer Datenschutzunterstützung einen wesentlichen Schwerpunkt der Diplomarbeit darstellt, ist es notwendig, Lernmanagement-Systeme auch von anderen Formen des computerunterstützten Lernens und Lehrens abzugrenzen. Auf diese Weise soll eine eindeutige Unterscheidung zu andere Techniken und Produkte ermöglicht werden.

Grundsätzlich bezeichnet der Begriff Lernmanagement-System bestimmte Softwareprodukte, die zur Unterstützung der (Unterrichts-)Lehre eingesetzt werden. Da die Entwicklung an derartiger Lernsoftware nie vollständig abgeschlossen ist, sie also ständig weiterentwickelt und im Umfang erweitert wird, ist eine präzise und allgemeingültige Definition von Lernmanagement-Systemen nicht ohne weiteres möglich. Dennoch sollen im Folgenden einige Definitionen zu Lernmanagement-Systemen vorgestellt und miteinander verglichen werden.

Als erstes sei eine entsprechende Definition von Baumgartner et al. genannt [Bau02]. Eine Definition von Lernmanagement-Systemen, die bei Baumgartner auch als „webbasierte Lernplattformen“ bezeichnet werden, basiert auf der Bestimmung grundlegender Funktionen, durch die die Autoren den Umfang dieser Systeme beschreiben. So untergliedern Baumgartner et al. die Funktionen eines Lernmanagement-Systems in die folgenden fünf Bereiche [Bau02]:

- Präsentation von multimedialen Inhalten,
- Werkzeuge für synchrone und asynchrone Kommunikation,
- Werkzeuge zur Erstellung von Aufgaben und Übungen,
- Evaluations- und Bewertungshilfen,
- Administration von Lernenden, Inhalten, Kursen, Lernfortschritten und Terminen.

Die genannten Funktionsbereiche sollen als Grundorientierung für eine Charakterisierung dienen. Dabei legen die Autoren besonderen Wert auf eine Integration von Werkzeugen, die

das Lehren und Kommunizieren innerhalb einer Lernplattform ermöglichen beziehungsweise vereinfachen sollen. Des Weiteren werden Funktionen, die das Bewerten und Evaluieren unterstützen, von den Autoren als ein grundlegender Funktionsbereich dargestellt. Auch die Inhaltspräsentation und Administration von Objekten und Teilnehmern wird als wesentlich für ein Lernmanagement-System angesehen.

Baumgartner et al. verstehen demnach unter einem Lernmanagement-System „*eine serverseitig installierte Software […], die beliebige Lerninhalte über das Internet zu vermitteln hilft und die Organisation der dabei notwendigen Lernprozesse unterstützt*." [Bau02]

Von den Autoren wird weiterhin eine Unterteilung der Lernmanagement-Systeme hinsichtlich ihres unterstützten Lernansatzes vorgenommen. Dabei wird einerseits in den lehrerzentrierten Ansatz unterteilt, der dem klassischen Unterricht nachempfunden ist und in den lernerzentrierten Ansatz, in dem das selbstgestaltete Lernen gefördert wird. Bei der Unterscheidung ist weniger der Funktionsumfang eines Lernmanagement-Systems ausschlaggebend als vielmehr die Berechtigungen, wem bestimmte Funktionen in welchem Umfang letztendlich zur Verfügung stehen. So ist beispielsweise eine Chatfunktion, die nur eine Kommunikation zwischen Lehrenden und Schülern ermöglicht, nicht aber zwischen Schülern untereinander, ein lehrerzentrierter Ansatz.

Eine weitere Definition für Lernmanagement-Systeme stammt von Brandon Hall [Hal07]. Er definiert Lernmanagement-System folgendermaßen:

"A Learning Management System, or LMS, is software that automates the administration of training events. All LMSs manage the log-in and registration of users, manage course catalogs, record data from learners, and provide reports to management."

Die Hauptaufgaben eines Lernmanagement-Systems werden hier in der Automatisierung der Administration des Lehrbetriebes und in der Verwaltung von Benutzern und Kursinhalten gesehen. Außerdem stellen die Speicherung von Lernaktivitäten und das Erstellen von Dokumentationen weitere Funktionen von Lernmanagement-Systemen dar.
Hall geht davon aus, dass unter dem Begriff Lernmanagement-System vielerlei Applikationen fallen, die den Lernprozess mitverfolgen und die folgenden Funktionen optional unterstützen können:

- Autorenwerkzeuge,
- Management von Studiengruppen,
- Kompetenzmanagement,
- Wissensmanagement,
- Zertifizierung und Mitarbeiterschulungen,
- Personalisierung,
- Betreuung,
- Chat,
- Diskussionsforum.

Hall fügt seiner Definition somit zusätzliche Funktionen hinzu, die insbesondere Managementaufgaben und die Betreuung der Lernenden beinhalten.

Auch Schulmeister definiert in [Sch05] Lernmanagement-Systeme aufgrund des Umfanges ihrer Funktionalitäten. So werden Software-Systeme, die über folgende Funktionen verfügen als Lernmanagement-System angesehen:

- Benutzerverwaltung,
- Kursverwaltung,
- Vergabe von Rollen und Rechten,
- Kommunikationsmethoden und Werkzeuge für das Lernen,
- Darstellung von Lerninhalten, Lernobjekten und Medien über das Internet.

Bezugnehmend auf die Definition von Baumgartner verwendet Schulmeister einen etwas abgeänderten Funktionsumfang für ein Lernmanagement-System und nimmt insbesondere die Verteilung von Rollen und eine differenzierte Rechtevergabe auf.

Um die Definition eines Lernmanagement-Systems weiter zu konkretisieren, stellt Schulmeister in einem Schema (siehe Abbildung 2.1) den Aufbau einer Lernmanagement-System-Architektur grafisch dar. In diesem Diagramm nimmt er eine Einteilung in drei verschiedene Schichten vor, in die die wichtigsten Elemente eines Lernmanagement-Systems eingeordnet werden.
Die Datenbankschicht, die im unteren Abschnitt der Abbildung dargestellt wird, ist für die Haltung von Lernobjekten und Benutzerdaten verantwortlich. Die darauf liegende Schicht beinhaltet Schnittstellendefinitionen zu anderen Systemen wie beispielsweise Abrechnungssystemen, Verschlüsselungskomponenten, Studenten- oder Raumverwaltungen. Bei manchen Lernmanagement-Systemen werden auch Komponenten ausgegliedert, die Evaluation und Statistik unterstützen, Autorenwerkzeuge oder spezielle Kommunikationsmethoden bereitstellen. Diese sind dann nur über API-Schnittstellen zu externen Programmen verfügbar. Ebenfalls existieren Lernmanagement-Systeme, die die Haltung von Lernobjekten außerhalb des Systems vorsehen.

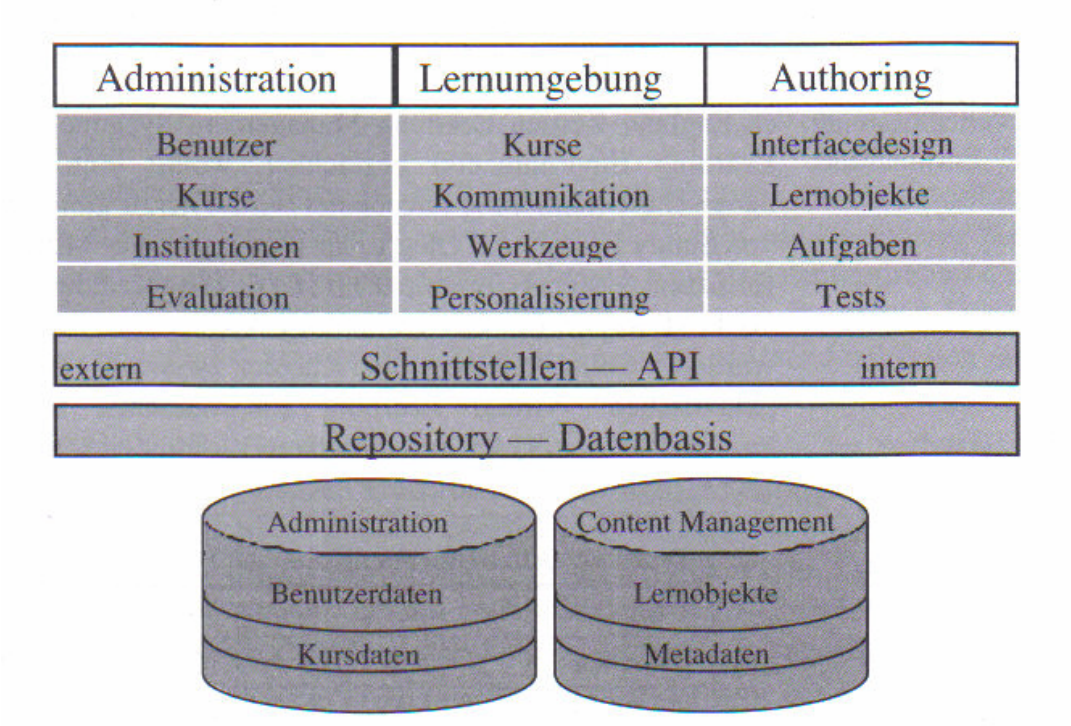

Abbildung 2.1: Idealtypische Architektur eines Lernmanagement-Systems aus [Sch05]

Die oberste Schicht dient der Darstellung von Inhalten und Funktionen für Lehrende, Lernende und Administratoren. Dazu gehören nach Abbildung 2.1 Funktionen der Administration, um Benutzer, Kurse und Institutionen zu verwalten. Außerdem werden hier die Evaluationsmethoden eingeordnet. Der Bereich der Lernumgebung beinhaltet Objekte und Anwendungen, die der Lehrstoffvermittlung dienen sollen. Hier sind die Kurse, Kommunikationswerkzeuge, Werkzeuge für Lernende, beispielsweise um Notizen anzulegen und eine personalisierte Unterstützung der einzelnen Lernenden zu nennen. Im Authoring-Bereich stehen Werkzeuge zur Verfügung, um Lernobjekte, Aufgaben und Tests zu erstellen. Außerdem kann hier das Interface der Lernplattform verändert werden.

Zusammenfassend gibt Schulmeister eine eng gefasste Definition bezüglich der vorhandenen Funktionen, die aber nicht detaillierter auf die Ausgestaltung und die Komplexität der einzelnen Funktionen eingeht. Es ist aber eine Abgrenzung zu folgenden verwandten Systemen durch seine Definition möglich:

- Reine Autorenwerkzeuge,
- Spezialisierte Kommunikationsmethoden,
- Virtuelle Klassenräume mit geringer Verwaltungsfunktion,
- Bildungsinhalte, die keine organisierenden Funktionen für den Lernprozess anbieten,
- Management-Syteme, die keine inhaltlichen Funktionen für den Lernprozess anbieten,
- Contentmanagement-Systeme, die über keine Steuerung des Lernprozesses verfügen,
- Andere webbasierte Systeme, die neben ihrem eigentlichen Zweck auch zu Lernzwecken verwendet werden können. Dazu gehören Application Sharing und Dateiaustauschprogramme wie das BSCW.

Im europäischen Raum wird neben dem Begriff des Lernmanagement-Systems auch der Begriff *Virtual Learning Environment* (Virtuelle Lernumgebung, VLE) verwendet. Dieser kann bis zu einem gewissen Maß mit dem des Lernmanagement-Systems gleichgesetzt werden [Sch05]. Dabei orientiert sich die Definition der *Virtual Learning Environment* aber eher an pädagogischen Eigenschaften.

Ausgehend von der Analyse untersuchter Lernplattformen schlussfolgert Schulmeister, dass es den Trend gibt, ein klassisches Lernmanagement-System um ein Contentmanagement-System zu erweitern. Auf diese Weise wird es einfacher Kurse und Inhalte von Lernmanagement-Systemen zu verwalten. Für den neu entstandenen Systemverbund wurde die Bezeichnung *Learning Content Management System*, kurz LCMS, geprägt.

2.2 Auswahl von State-of-the-Art Lernmanagement-Systemen

Aufgrund des Umstandes, dass es keine global eindeutige Definition für ein Lernmanagement-System gibt, liegt die Zuordnung der einzelnen Vertreter in erster Linie bei den Herstellern selbst. Eine derartige, subjektive Klassifikation führt dann dazu, dass bei Untersuchungen wie in [Sch05] und [Bau02] die Autoren einige der als Lernmanagement-System angebotenen Produkte aus der Evaluation ausschließen mussten, da sie nicht den jeweilig aufgestellten Definitionen für Lernmanagement-Systemen entsprachen.

Bei der von Baumgartner et al. 2002 durchgeführten Untersuchung wurden beispielsweise zunächst 133 potentielle Lernmanagement-Systeme ermittelt. Diese Anzahl musste aber korrigiert werden, da einige lediglich unter verschiedenen Namen angeboten wurden. Weitere 16

Produkte konnten nach genauerer Betrachtung nicht als Lernmanagement-System eingeordnet werden. So konnten letztendlich nur 89 Produkte als Lernmanagement-System identifiziert und einer weiteren Benutachtung unterzogen wurden.
Schulmeister hat im Dezember 2001 bei einer ähnlichen Recherche 171 Systeme ermittelt, die als Lernmanagement-Systeme eingestuft werden könnten. Dabei geht auch Schulmeister davon aus, dass in der Vielzahl der gefundenen Systeme Produkte enthalten sind, die von den Herstellern auf ihrer Webseite zwar als Lernmanagement-System bezeichnet werden, diese aber keine vollständigen Lernmanagement-Systeme sind. Weiterhin nimmt er aber auch an, dass nicht alle Lernmanagement-Systeme, die weltweit eingesetzt werden, in der Recherche enthalten sind. Es wird jedoch von ihm davon ausgegangen, dass die leistungsfähigsten Vertreter dieser Softwarekategorie in seiner Untersuchung einbezogen wurden. Auch Brandon Hall hat 2001 eine Marktanalyse von Lernmanagement-Systemen veröffentlicht, in der 72 Vertreter enthalten sind [Sch05]. Dabei wurden aber auch kommerzielle Produkte mit einbezogen, die vornehmlich für die betriebliche Weiterbildung konzipiert wurden.

Es gibt also bislang keine einheitliche Definition für Lernmanagement-Systeme. Folglich kommt es je nach Definition zu stark variierenden Zahlenangaben der am Weltmarkt befindlichen Lernmanagement-Systeme. Je nachdem wie weit oder eng die Definition gefasst ist, kann man von einigen Dutzend bis zu mehreren hundert Produkten ausgehen.
Ein weiteres Problem gestaltet sich in der kurzen Aktualität derartiger Übersichten, wie sie von Schulmeister und Baumgartner et al. angefertigt wurden. Der Herstellermarkt ist relativ groß und sehr dynamisch. So gab Schulmeister dies selbst zu bedenken, da direkt nach seiner durchgeführten Recherche Produkte wieder verschwunden waren, aufgekauft wurden oder weitere hinzugekommen waren.

Aktuelle und repräsentative Marktanalysen konnten nach eingehender Recherche nicht ermittelt werden. Einen Einblick in die Situation, welche Lernmanagement-Systeme in welchem Umfang verwendet werden, kann nur fragmentarisch aus Umfragen und Veröffentlichungen gewonnen werden. Auch hat das OpenSource-Angebot von Lernmanagement-Systemen stark zugenommen, so dass die Produkte, die 2001 beziehungsweise 2002 verwendet wurden, nun durch kostengünstigere Systeme ersetzt werden können.

Um zu ermitteln, welche Lernmanagement-Systeme für die eigene Analyse verwendet werden sollen, wurden Quellen aus den letzten fünf Jahren hinzugezogen. Diese beziehen sich entweder auf Recherchen des Lernmanagement-System-Marktes und auf Bewertungsverfahren, bei denen Lernmanagement-Systeme nach Bewertungskriterien beurteilt wurden. Oder sie stützen sich auf Ergebnisse aus Umfragen, welche Lernmanagement-Systeme derzeit häufig genutzt werden, also einen umfangreichen Benutzerkreis aufweisen. Unter Beachtung all der genannten Faktoren sollen diejenigen Lernmanagement-Systeme extrahiert werden, die in der Summe in den meisten Quellen positiv vertreten sind.

Die Tabellen 2.1 und 2.2 stellen die Ergebnisse aus Baumgartner et al. und Schulmeister in Verbindung mit neueren Untersuchungen in diesem Umfeld dar. Dabei werden die Lernmanagement-Systeme aufgeführt, welche laut den durchgeführten Untersuchungen als besonders praktikabel beziehungsweise verbreitet angegeben wurden. Diese Faktoren sollen implizit die Güte und damit State-of-the-Art repräsentieren.

Betrachtet man die Tabellen 2.1 und 2.2 genauer, so fällt auf, dass einige Systeme in vielen der aufgeführten Quellen enthalten sind. Im Bereich der kommerziellen Systeme sind dies unter anderem Blackboard und WebCT, außerdem kommen CLIX, Lotus Learning Space,

Saba Enterprise Learning Suite und Top Class überdurchschnittlich häufig vor. Für eine eingehende Untersuchung sollen besonders die Systeme WebCT und Blackboard als Vertreter

LMS:	Anbieter:	Paulsen 2002 [1]	Baumgartner 2002[2]	Schulmeister 2003[3]	Frauenhofer 2003[4]	Wyles 2004[5]	Baumgartner 2005[6]	Wild 2006[7]	Stange 2006[8]	Σ
Kommerzielle Systeme										
Aspen	Click2Learn				x					1
Blackboard	**Blackboard**	**x**	**x**				**x**	**x**	**x**	**5**
ClassFronter		x								1
Campus 2000 Online	Ibis acam Partner AG		x							1
Clix	**IMC GmbH**		**x**	**x**			**x**		**x**	**4**
Distance Learning System	ETS GmbH		x		x		x			3
Discendum Optima								x		1
Docent	Docent Inc.		x							1
eDoceo								x		1
eLearning Suite	Hyperwave		x				x		x	3
Enterprise Learning Platform	Sun Microsystems		x							1
FirstClass		x							x	2
IBT Server	Time4you GmbH		x	x			x			3
iLearning	Oracle		x		x		x			3
IntraLearn	IntraLearn			x	x					2
Learning Space	**Lotus/IBM**	**x**	**x**				**x**		**x**	**4**
LUVIT		x								1
Saba Enterprise Learning Suite	**Saba**		**x**	**x**	**x**		**x**			**4**

Tabelle 2.1: Vergleich von Lernmanagement-Systemen (Teil 1)

[1] [Pau02] Die am meisten genutzten, kommerziellen Lernmanagement-Systeme in Europa.
[2] [Bau02] Die Top 16 Lernmanagement-Systeme, ermittelt von Peter Baumgartner, Hartmut Häfele und Kornelia Maier-Häfele.
[3] [Sch05] Schulmeister hat für die Auswahl eines geeigneten Lernmanagement-Systems für einen konkreten Anwendungsfall fünf Systeme in die nähere Auswahl genommen, die seine in [Sch05] genannten Kriterien am besten erfüllen.
[4] [Het03] Kommerzielle Systeme, die mindestens mit 150 Installationen weltweit angegeben werden.
[5] [Wyl04] führende OpenSource-Systeme.
[6] [Hae05] Top 16 Lernmanagement-Systeme.
[7] [Wil06] Europaweite Befragung von Hochschulen und Universitäten zu genutzter Lernsoftware; nur Systeme, die mehr als zweimal auftraten, wurden in der Übersicht berücksichtigt.
[8] [Sta06] Europaweite Umfrage zu Datenschutz und Privatheit im eLearning; nur Lernmanagement-Systeme, die mindestens zweimal angegeben wurden, wurden in der Übersicht berücksichtigt.

LMS:	Anbieter:	Paulsen 2002	Baum-gartner 2002	Schul-meister 2003	Frauen-hofer 2003	Wyles 2004	Baum-gartner 2005	Wild 2006	Stange 2006	Σ
Sitos	Bitmedia		x				x			2
Thinktanx	Viviance GmbH		x							1
Top Class	**WBT-Systems**	**x**	**x**		**x**		**x**			**4**
Tutor2000		x								1
Viversa	Viwis Gmbh						x			1
WebCT	**WebCT**	**x**	**x**	**x**			**x**	**x**	**x**	**6**
OpenSource-Systeme										
ATutor	Uni To-ronto					x	x			2
Chef						x				1
Claroline	Uni Lou-vain					x	x			2
DotLRN						x				1
ILIAS	**Uni Köln**		**x**			**x**	**x**		**x**	**4**
It's Learn-ing									x	1
Moodle	**Mood-le.com**					**x**	**x**	**x**	**x**	**4**
Stud.IP									x	1
BluES'n	**TU Dres-den**								**x**	**1**

Tabelle 2.2: Vergleich von Lernmanagement-Systemen (Teil 2)

kommerzieller Systeme betrachtet werden. Außerdem soll als drittes Lernmanagement-System noch CLIX hinzugenommen werden, da auch dieses Lernmanagement-System in jüngsten Umfragen angegeben wird und somit von einer aktuellen Nutzung und einer guten Marktposition dieses Systems auszugehen ist. Die Systeme Moodle und Ilias werden als Vertreter des OpenSource-Bereiches in den Quellen oft positiv hervorgehoben oder weisen eine hohe Verbreitung auf. Diese Beobachtung stimmt auch mit den in [Sta06] gewonnenen Ergebnissen überein und soll daher als Ausgangspunkt für die durchzuführende Betrachtung des OpenSource-Sektors dienen. Neben diesen Produkten sollen ebenfalls das OpenSource-System OLAT, das vom Bildungsportal Sachsen angeboten wird und BluES'n, das derzeit an der Technischen Universität Dresden entwickelt wird, betrachtet werden. Bei diesen Produkten ist insbesondere durch die Nähe zu Anbietern und Entwicklern eine besonders intensive Analyse möglich.

2.3 Abgrenzung des Untersuchungsgebietes

In diesem Abschnitt soll der Rahmen der eigenen Untersuchung festgelegt werden. Aus den vorgestellten Definitionen lässt sich entnehmen, dass das Untersuchungsgebiet sehr weitläufig sein kann, wenn man alle möglichen Komponenten betrachtet, die über externe und interne Schnittstellen an das Lernmanagement-System angebunden werden können. Außerdem wird in der in Abbildung 2.1 vorgestellten Architektur eines Lernmanagement-Systems auch die Datenhaltung einbezogen. Dazu kommen weitere technische Vorraussetzungen, die den Datenschutz beeinflussen können, wie zum Beispiel das darunter liegende Betriebssystem, der Webserver und die Datenbank. Auch durch den verteilten Zugriff auf ein Lernmanagement-System, der meist über das Internet getätigt wird, sind alle Gefahren, die beispielsweise bei

einem eCommerce-Angebot im Internet eintreten können, auch bei einer verteilten Lernanwendung vorhanden. Bei der dabei meist verwendeten dreischichtigen Architektur, siehe Abbildung 2.2, benötigt der Client nur einen Browser, um ein Angebot, das über einen Server zur Verfügung gestellt wird, zu nutzen. Serverseitig stellt der *Web Server* die Repräsentation aller Komponenten, wie Inhalt und Benutzereingaben, zur Verfügung. Der *Application Server* verarbeitet die Benutzereingaben und übernimmt die Datenverarbeitung. In der *Database* werden Daten abgespeichert und bei Bedarf wieder geladen. Insbesondere kann hier auch der Kommunikationsweg, über den Daten übermittelt werden, einen Schwachpunkt für den Datenschutz darstellen. Weippl stellt in seinem Buch *Security in e-Learning* [Wei05] eine Übersicht auf, die mögliche Gefahren an Stationen der Kommunikation über das Internet darstellt. Diese Gefahren können bei einer Übermittlung von Daten die Sicherheit und den Datenschutz beeinträchtigen. Die genannte Übersicht ist nochmals in Abbildung 2.4 dargestellt. Wie zu erkennen ist, kann schon auf dem Computer des Benutzers Software installiert sein, die Aufzeichnungen von Eingaben oder des Bildschirms vornehmen, wie *Keylogger* oder *Screen Scrapers.* Im weiteren Verlauf der Übertragung können beispielsweise durch das Aufzeichnen der IP-Adresse und der Webseiten, die in der Lernplattform aufgerufen werden, durch Dritte Verhaltensprofile erstellt werden.

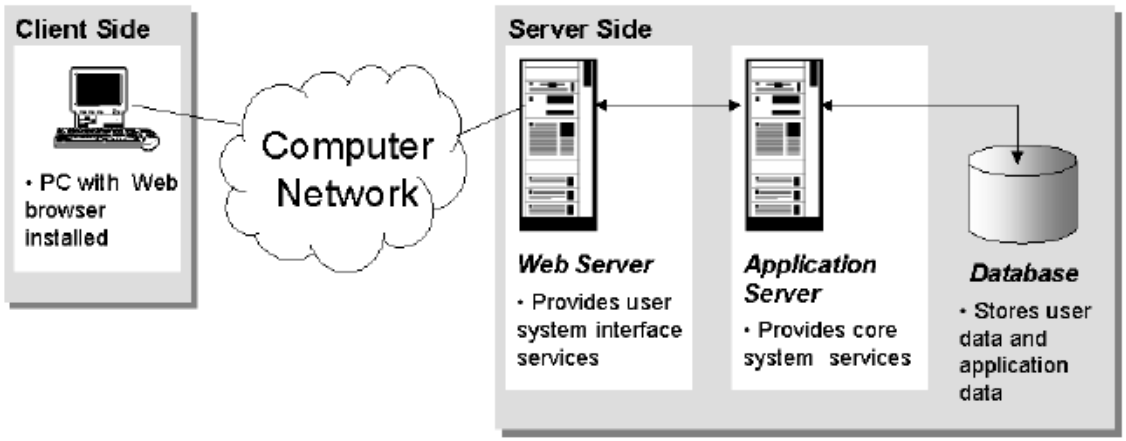

Abbildung 2.2: Dreischichtige Architektur aus [Cha03]

Ein weiterer wichtiger Bereich, der den Datenschutz beeinträchtigen kann, sind die organisatorischen Maßnahmen und die Sensibilisierung der Personen oder Mitarbeiter, die Zugriff auf die technischen Sicherheits- und Datenschutzmaßnahmen haben. Nur wenn die bereitgestellten Möglichkeiten zum Datenschutz auch wahrgenommen werden, können diese auch sinnvoll eingesetzt werden.

Aus den vorgestellten Umgebungskriterien, die den Datenschutz eines Lernmanagement-Systems beeinflussen können, kann die folgende Abbildung 2.3 erstellt werden. Anhand dieser sollen auch die Untersuchungsschwerpunkte der Diplomarbeit erläutert werden.

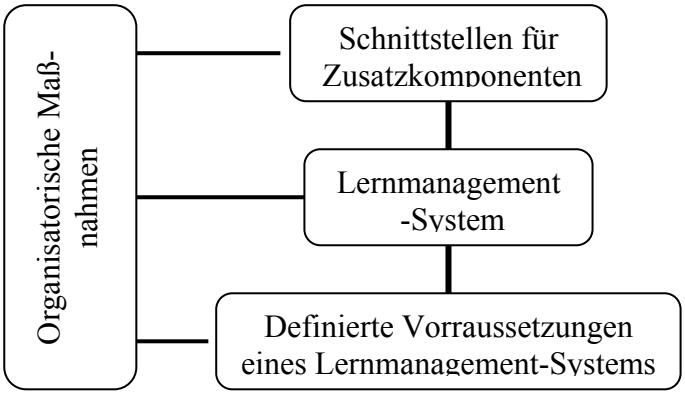

Abbildung 2.3: Das sicherheits- und datenschutzrelevante Umfeld eines Lernmanagement-Systems

Definierte Vorraussetzungen eines Lernmanagement-Systems: Wie schon angesprochen, benötigt ein Lernmanagement-System für die Inbetriebnahme ein Betriebssystem, einen Webserver und in den meisten Fällen auch eine Datenbank. Dabei kann eine Lernplattform meist mehrere Betriebssysteme, Webserver- und Datenbanksoftware unterstützen. Je nach benötigten Betriebssystem und Software kann es auch sicherheits- und datenschutzrelevante Unterschiede geben. Da derartige Software Voraussetzung für ein lauffähiges Lernmanagement-System ist, aber nicht direkt Bestandteil dieses, werden diese in der Arbeit nicht betrachtet. Bietet eine Lernplattform beispielsweise eine eigene Datenhaltung an, soll diese aber in die Untersuchung einfließen.

Lernmanagement-System: Das Lernmanagement-System an sich umfasst die Funktionen, Dienste, Einstellungen und Sicherheitskonzepte, die direkt in die Lernplattform integriert sind beziehungsweise, bei modularem Aufbau, zusammen mit der Hauptkomponente angeboten werden. Hier soll auch betrachtet werden, ob und welche Standards die Lernplattform unterstützt, welche Konfigurationen aus Sicht des Datenschutzes vorgenommen werden können und welche Standardeinstellungen voreingestellt sind.
So sollen insgesamt Funktionen, die in Abbildung 2.1 als oberste Schicht eines Lernmanagement-Systems charakterisiert sind, das Hauptuntersuchungsgebiet dieser Arbeit darstellen. Hierzu gehören insbesondere die Administration, das Authoring und die Lernumgebung,

Schnittstellen für Zusatzkomponenten: Weitere Komponenten, die nicht unter Lernmanagement-System aufgeführt sind, sollen nicht in die Untersuchung einbezogen werden.

Organisatorische Maßnahmen: Hierzu gehören Vorkehrungen, die außerhalb der Softwareumgebung getroffen werden, um den Datenschutz zu unterstützen. Das kann sich zum Beispiel auf die grundlegende Sensibilisierung von Mitarbeitern, insbesondere Systemadministratoren, beziehen. Diese sind für die Konfiguration des Softwaresystems verantwortlich und können dadurch als „Schlüsselfigur“ für die Realisierung des Datenschutzes betrachtet werden. Auch die Sicherheits- und Datenschutzvorkehrungen innerhalb der Organisation, die eine Lernplattform betreibt, sind hier von Relevanz sowie der physikalische Schutz des Systems. Ob und wie datenschutzrelevante Funktionen einer Lernplattform eingesetzt werden, ist meist von den organisatorischen Maßnahmen abhängig. Da sich die Datenschutzbewertung auf Lernmanagement-Systeme bezieht, sollen die organisatorischen Vorkehrungen

nur am Rande betrachtet werden. Auch da davon auszugehen ist, dass ihre Umsetzung von Organisation zu Organisation variiert und kaum von der Lernplattform beeinflusst werden kann. Ob sich bei einer konkreten Installation die organisatorischen Maßnahmen von den Fähigkeiten des jeweiligen Lernmanagement-Systems isolieren lassen, muss in der Durchführung der Bewertung ermittelt werden.

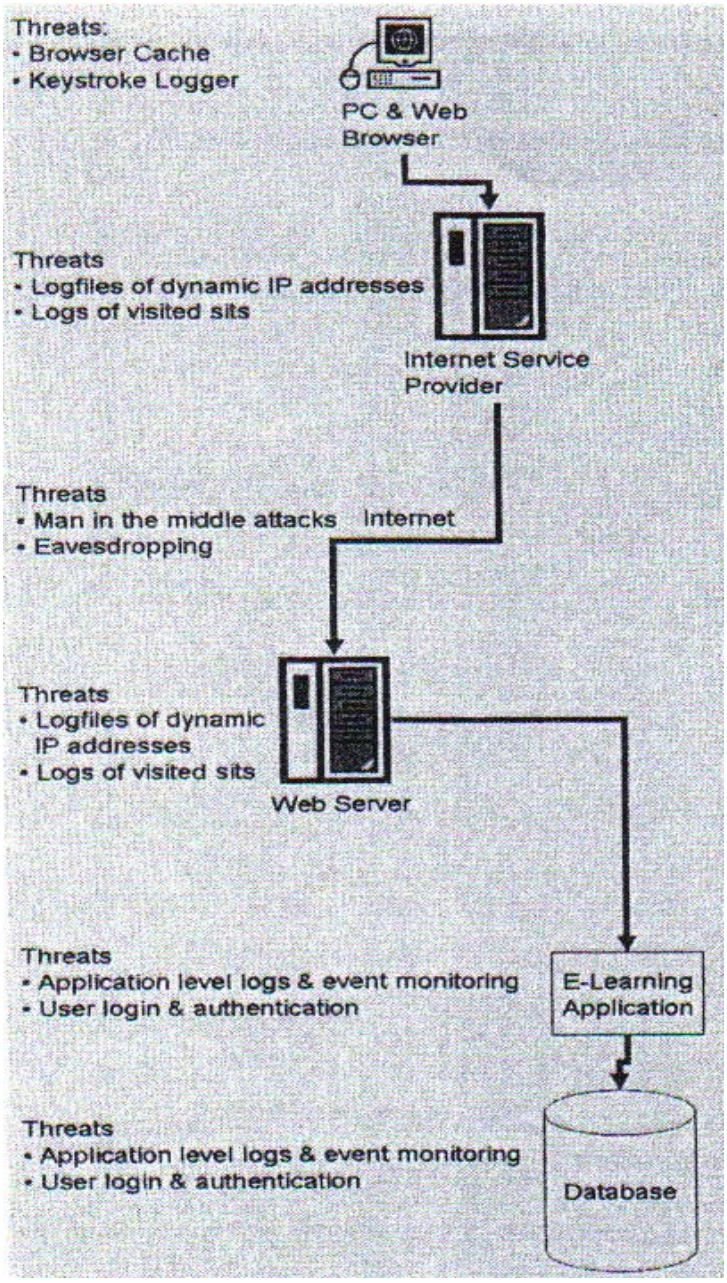

Abbildung 2.4: Gefahren für den Datenschutz und die Datensicherheit, die bei der Übermittlung von Daten über das Internet auftreten können (aus [Wei05]).

2.4 Zusammenfassung

In diesem Kapitel wurden Definitionen von Lernmanagement-Systemen vorgestellt, die zeigen, dass bestimmte Vorstellungen zum Funktionsumfang bei vielen Quellen übereinstimmen, aber es auch zu leichten Variationen bei den Anforderungen kommt. Meist ist die Definition eines Lernmanagement-Systems daran geknüpft, was den Autoren für eine Bewertung oder Auswahl von Lernplattformen wichtig ist.

Für die Auswahl von Lernmanagement-Systemen, die für die weitere Untersuchung und Bewertung von Lernmanagement-Systemen zu betrachten sind, ist eine konkrete Definition der Softwaresysteme, welche man als Lernmanagement-Systeme bezeichnen kann, erforderlich. Die weitere Arbeit soll sich dabei auf die Definition von Schulmeister beziehen und die Funktion für „Evaluations- und Bewertungshilfen“ von Baumgartner et al. hinzunehmen. Damit ist ein Großteil des Funktionsumfangs abgedeckt:

- Benutzerverwaltung,
- Kursverwaltung,
- Vergabe von Rollen und Rechten,
- Kommunikationsmethoden und Werkzeuge für das Lernen,
- Evaluations- und Bewertungshilfen,
- Darstellung von Lerninhalten, Lernobjekten und Medien über das Internet.

Eine Auswahl der zu untersuchenden Lernmanagement-Systeme wurde im zweiten Abschnitt vorgenommen. Anhand von mehreren Einflussfaktoren aus unterschiedlichsten Quellen wurden sieben Lernmanagement-Systeme ausgewählt. Dabei wurde eine Unterscheidung in kommerzielle und OpenSource-Systeme vorgenommen. Darüber hinaus wurde das prototypische System BluES’n in die Datenschutzbewertung aufgenommen.

Im dritten Abschnitt wurde der Rahmen der Datenschutzuntersuchung von Lernmanagement-Systemen ermittelt. So werden weder die definierten Vorraussetzungen für die Inbetriebnahme eines Lernmanagement-Systems untersucht noch Zusatzsoftware, die nicht mit der Hauptkomponente angeboten wird. Genauer sollen die eigentlichen Funktionen eines Lernmanagement-Systems untersucht werden, wobei die organisatorischen Maßnahmen am Rande betrachtet werden sollen.

3. Gesetzliche Grundlagen zum Datenschutz und der Informationellen Selbstbestimmung

Im folgenden Kapitel werden die grundlegenden Gesetze zur Handhabung von personenbezogenen Daten und der Gewährleistung der Selbstbestimmung über diese Daten eingehend erläutert. Insbesondere sollen dabei die Gesetzgebungen des europäischen Raums vorgestellt werden.
Begonnen wird im ersten Abschnitt mit der Betrachtung internationaler Richtlinien, wie die des Europarates, der OECD und der Europäischen Gemeinschaft. Insbesondere wird hier auf die EU-Leitlinien 95/46/EG und 2002/58/EG eingegangen. Im Anschluss daran führt die Betrachtung hin zu nationalen Datenschutzgesetzen, die am Beispiel der deutschen Datenschutzgesetzgebung vorgestellt werden. Auch eine Betrachtung des Datenschutzes im Bereich eLearning und der Hochschulen wird vorgenommen. Im Weiteren wird der Datenschutz im Hinblick auf Minderjährige betrachtet. Im Mittelpunkt stehen dabei Gesetze, die sich mit dem speziellen Thema der Verarbeitung von personenbezogenen Daten bei Jugendlichen beschäftigen. Dazu gehört der *Family Educational Rights and Privacy Act* (FERPA), welches in den Vereinigten Staaten die Grundlage zur Handhabung von Informationen über Jugendliche und Studenten bildet. Abschließend sollen durch die Gesetze aus den vorgestellten Bereichen Schlussfolgerungen für die weitere Arbeit diskutiert werden.

3.1 Internationale Regelungen

3.1.1 Europarat

Das Recht eines Individuums auf Privatheit ist 1950 als eines der Grundrechte in der *Konvention zum Schutz der Menschenrechte und Grundfreiheiten* (EMRK) durch den Europarat verabschiedet worden. Dabei wurden in der Konvention schon Bereiche der Privatheit unterschieden, die die lokalen, informationellen, physischen und relationalen Aspekte einbeziehen [EMRK].
Wirtschaftliche Verflechtungen über die Grenzen einzelner Länder hinweg nahmen seitdem stetig zu und auch die Datenverarbeitung mit Hilfe von Computern setzte ein. Dies hatte zur Folge, dass auch personenbezogene Daten über Ländergrenzen hinweg ausgetauscht und Datenbanken aus unterschiedlichen Ländern miteinander verknüpft werden sollten. Auf internationaler Ebene waren einheitliche Regelungen für die Gewährleistung des Datenschutzes nicht vorhanden, so dass hier Richtlinien für einen grenzüberschreitenden Datenschutz erarbeitet werden mussten.

Der Europarat stellte 1981 das „*Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten*“ (Konvention Nr. 108) [Kon81] vor.
In dieser sollte, wie auch bei den Datenschutzrichtlinien der OECD (siehe Abschnitt 3.1.2), ein einheitliches Datenschutzniveau in den Mitgliedsstaaten geschaffen werden, das den grenzüberschreitenden Datenverkehr nicht behindert. Der Datenschutz soll dabei anhand der Grundsätze der Datenverarbeitung „nach Treu und Glauben“, der „Zweckbindung“, der „Erforderlichkeit“ sowie durch den „Informationsanspruch des Betroffenen“ gewährleistet werden [Kon81]. Anders als bei der Datenschutzrichtlinie der OECD beinhaltet die Konvention aber die Verpflichtung, die Bestimmungen in nationales Recht zu überführen.
Dabei liegt der Fokus auf der Gewährleistung der Informationsübermittlung zwischen den Mitgliedsstaaten, was sich insbesondere in dem Verbot widerspiegelt, eine Datenübertragung

allein aus Gründen des Datenschutzes zu verhindern. So bleibt auf Basis der Konvention das Datenschutzniveau niedrig, da es sich dem Mitgliedstaat mit den geringsten Datenschutzanforderungen anpasst [Lav96].

3.1.2 OECD

Die OECD (Organisation für Wirtschaftliche Zusammenarbeit und Entwicklung) veröffentlichte 1980 Richtlinien, um die informationelle Privatheit zu schützen und stellte damit einen wichtigen Ansatz für die Umsetzung von Datenschutzbestimmungen zur Verfügung [OECD]. In ihren Richtlinien aber spricht die OECD nur unverbindliche Empfehlungen aus, wie sensitive Daten zu schützen sind. Somit wird keine Realisierung dieser Leitlinien innerhalb der Mitgliedsstaaten durch die OECD durchgesetzt.
Folgende acht Grundsätze für eine angemessene Umsetzung des Datenschutzes wurden durch die OECD aufgestellt:

- Grundsatz der begrenzten Datenerhebung,
- Grundsatz der Datenqualität,
- Grundsatz der Zweckbestimmung,
- Grundsatz der Nutzungsbegrenzung,
- Grundsatz der Sicherung,
- Grundsatz der Offenheit,
- Grundsatz des Mitspracherechts,
- Grundsatz der Rechenschaftspflicht.

Der Schwerpunkt dieser Richtlinien liegt dabei auf der Vereinfachung des internationalen Austauschs von personenbezogenen Daten und die Gewährleistung eines sicheren Datenverkehrs in andere Mitgliedsstaaten.

3.1.3 Europäische Gemeinschaft

Für den Bereich der Europäischen Gemeinschaft werden nun die EU-Richtlinien 95/46/EG und 2002/58/EG vorgestellt. Diese stellen die Vorgaben der Europäischen Gemeinschaft hinsichtlich des Datenschutzes dar. Jeder Mitgliedsstaat ist dazu verpflichtet, diese EU-Richtlinien in die Gesetzgebung des jeweiligen Landes zu übertragen. So werden die Gesetzgebungen der einzelnen Länder harmonisiert. Bei der Umsetzung der jeweiligen Richtlinien sind aber den einzelnen Ländern noch gewisse Handlungsspielräume gegeben, sodass es zu leichten Varianzen bei der Umsetzung in den einzelnen Mitgliedsstaaten kommt.

Die 1995 verabschiedete *Datenschutzrichtlinie des europäischen Parlamentes und des Rates* sieht den „Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ [EUR95] vor. Sie wird auch als Datenschutzdirektive 95/46/EG bezeichnet und bildet den Grundpfeiler der Datenschutzbestimmungen der Europäischen Gemeinschaft, indem es die Verarbeitung von personenbezogenen Informationen reguliert und das Recht auf Privatheit sicherstellt. Dabei orientiert sie sich an der Datenschutzkonvention des Europarates von 1981 und präzisiert die darin enthaltenen Richtlinien beziehungsweise fügt weitere hinzu.

Das Ziel der Europäischen Gemeinschaft ist somit die Gewährleistung grundlegender Datenschutzrechte und der Ausbau des Datenverkehrs im europäischen Binnenmarkt.

In der Direktive werden Grundprinzipien festgelegt, die bei der Datenerhebung und Verarbeitung von personenbezogenen Daten einzuhalten sind. Man versteht in diesem Zusammenhang unter „personenbezogenen Daten“*:*

> *„Alle Informationen über eine bestimmte oder bestimmbare natürliche Person (betroffene Person); als bestimmbar wird eine Person angesehen, die direkt, oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer, oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.“*
> (Artikel 2, Absatz a, 95/46/EG)

Die Datenschutzrichtlinie enthält wichtige Datenschutzgrundsätze, die nun vorgestellt werden sollen. Da die in der Datenschutzrichtlinie enthaltenen Datenschutzgrundsätze sehr umfangreich sind, werden diese im Folgenden nur gekürzt präsentiert [EUR95]:

- Rechtmäßigkeit der Verarbeitung personenbezogener Daten,
  - Qualität der Daten:
    - Die Datenverarbeitung soll nach Treu und Glauben erfolgen. Das heißt, wenn Daten erhoben werden, muss die betroffene Person in der Lage sein, das Vorhandensein einer Verarbeitung zu erfahren und ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert werden. Darüber hinaus soll die Datenverarbeitung auf rechtmäßige Weise durchgeführt werden.
    - Personenbezogne Daten werden für festgelegte, eindeutige und rechtmäßige Zwecke erhoben; dies beinhaltet die Zweckbestimmung und Nutzungsbegrenzung.
    - Personenbezogene Daten müssen dem Zweck entsprechen, für den sie erhoben wurden und/oder weiterverarbeitet werden, dafür erheblich sein und nicht darüber hinausgehen.
    - Personenbezogene Daten müssen sachlich richtig und wenn nötig aktuell sein.
    - Personenbezogene Daten dürfen nicht länger als für die Realisierung des Zwecks, für den sie erhoben wurden, in identifizierbarer Form gespeichert werden.
  - Zulässigkeit der Verarbeitung:
    - Für die Zulässigkeit der Datenverarbeitung muss eine der folgenden Vorraussetzungen erfüllt sein: Die betroffene Person hat ohne Zweifel ihre Einwilligung gegeben, das heißt ohne Zwang und mit Kenntnis der Sachlage, oder die Verarbeitung ist erforderlich für den Abschluss oder die Erfüllung eines für die betroffene Person bindenden Vertrages.
    - Die betroffene Person muss über die Datenverarbeitung informiert werden. Dabei müssen die Identität des für die Verarbeitung Verantwortlichen, die Zweckbestimmung der Verarbeitung, Empfänger oder Kategorien von Empfängern ersichtlich sein. Außerdem muss die betroffene Person über ihre Auskunfts- und Berichtigungsrechte infor-

miert werden und diese müssen durch den Verantwortlichen gewährleistet sein. Pflichten der Verantwortlichen sind die Gewährleistung der Datenqualität sowie der technischen Sicherheitsvoraussetzung.

  - Auskunftsrecht und Widerspruchsrecht der betroffenen Person: Sie hat das Recht auf Korrektur, Löschung oder Sperrung von inkorrekten oder illegal gespeicherten Daten. Personen, deren Daten Gegenstand der Verarbeitung sind, haben das Recht über diese informiert zu werden, Zugang zu den Daten zu erhalten, Berichtigung zu verlangen sowie Widerspruch gegen die Verarbeitung einzulegen.

- Vertraulichkeit und Sicherheit der Verarbeitung,

  - Die Vertraulichkeit der Datenverarbeitung muss gewährleistet werden.
  - Sicherheit: Derjenige, der die Daten kontrolliert, muss geeignete technische und organisatorische Sicherheitsmaßnamen durchführen, die den Schutz gegen die zufällige oder unrechtmäßige Verarbeitung gewährleisten. Insbesondere dann, wenn im Rahmen der Verarbeitung Daten in einem Netz übertragen werden. Bei der Einhaltung dieser Forderung ist unter Berücksichtigung des Standes der Technik und der bei ihrer Durchführung entstehenden Kosten durchzuführen, ein Schutzniveau zu gewährleisten, dass den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist. Hier ist die Integrität und Verfügbarkeit von personenbezogenen Daten zu garantieren.

Überwacht werden soll die Einhaltung der vorgestellten gesetzlichen Bestimmungen von unabhängigen Autoritäten. Deren Aufgabe ist es außerdem Beschwerden betroffener Personen nachzugehen.
Durch die dargestellte Richtlinie wird die Übertragung personenbezogener Daten in andere Länder außerhalb der Europäischen Union reguliert. Dabei darf nur bei Einhaltung angemessener Sicherheitsrichtlinien eine Übertragung in diese Länder stattgegeben werden. Ausreichender Schutz besteht beispielsweise bei Firmen aus den Vereinigten Staaten, die der Datenschutz-Vereinbarung „Safe-Harbor“[1] beigetreten sind.

Es hat etwa fünf Jahre gedauert, bis die europäische Datenschutzrichtlinie beschlossen wurde. In [Lav96] wird dies als geringes Interesse der Mitgliedsstaaten gewertet, einen wirksamen Datenschutz auf europäischer Ebene zu schaffen. Der Fokus der Richtlinie liegt demnach eher auf einem funktionierenden Binnenmarkt als auf der Gewährleistung eines wirkungsvollen Datenschutzes.

Eine weitere Richtlinie auf europäischer Ebene, die in diesem Zusammenhang kurz angesprochen werden soll, ist die *Datenschutzrichtlinie für elektronische Kommunikation* 2002/58/EG [EUR02]. Diese beinhaltet Regelungen, die die Verarbeitung von personenbezogenen Daten speziell im Telekommunikationssektor festlegen. Sie ergänzt die Richtlinie 95/46/EG mit Regelungen für den Datenschutz bei Telefongesprächen und der Verwendung von eMails.

Aus den bisherigen Erläuterungen zu Datenschutzgesetzen konnte feststellt werden, dass der Datenschutz zwar gesetzlich sichergestellt wird, aber sich vorrangig an wirtschaftlichen Ge-

[1] Siehe dazu URL: http://www.export.gov/safeharbor/

sichtspunkten orientiert und teilweise als Hindernis für einen freien Binnenmarkt angesehen wird [Lav96].
Die Datenschutzrichtlinien der EU gewähren einem Individuum, über seine personenbezogenen Daten selbst zu bestimmen. Die Einhaltung der Richtlinien ist aber nicht für Belange der öffentlichen Sicherheit und der Tätigkeiten des Staates im strafrechtlichen Bereich vorgeschrieben. Dieser Bereich der EU, der die Zusammenarbeit von Justiz und Polizei regelt, ist nicht zur Einhaltung der Richtlinien verpflichtet [Sha06]. Dies bedeutet, dass für die grenzüberschreitende Polizeiarbeit diese Gesetze keine Bedeutung besitzen.

Gegenwärtig wird durch Beschlüsse der Europäischen Union der Datenschutz anderen Interessen untergeordnet. Hier ist beispielsweise die Direktive zur Vorratsspeicherung 2006/24/EG [EUR06] zu nennen. Diese verpflichtet Anbieter von Telekommunikations- und Informationsdiensten elektronische Spuren zum Zweck der Vorratsdatenspeicherung bis zu 24 Monate zu speichern. Dies beinhaltet beispielsweise die Aufzeichnungen von Verbindungs- und Standortinformationen, die beim Telefonieren und im Internet anfallen. Die Datenspeicherung soll in erster Linie der Bekämpfung des Terrorismus und der Kriminalität dienen. So soll mit Hilfe der aufgezeichneten Daten das Kommunikationsverhalten und die Bewegungen von verdächtigen Personen verfolgt werden.
Grundsätzlich kann diese Direktive bedeuten, dass Informationen, die zur Strafverfolgung hinzugezogen werden können, enorm anwachsen und die Privatsphäre von allen Personen, die diese Dienste nutzen, beeinträchtigt wird [PRI06]. Der Europarat sieht in dieser Maßnahme zur wirksamen Strafverfolgung einen legitimen Grund, um das Recht auf Informationelle Selbstbestimmung einzuschränken. Dies bedeutet außerdem eine komplette Veränderung im Umgang mit personenbezogenen Daten. Sollte bisher nur soviel erhoben und verarbeitet werden, wie für einen bestimmten Zweck benötigt wird, wird in Zukunft soviel wie möglich aufgezeichnet werden [PRI06].

3.2 Nationale Datenschutzgesetze

Im Folgenden soll auf die nationale Datenschutzgesetzgebung eingegangen werden. Hierfür werden beispielhaft die Datenschutzgesetze Deutschlands herangezogen.

An erster Stelle soll hier das Volkszählungsurteil aus Deutschland genannt werden. Durch das Volkszählungsurteil [VZU] von 1983 des Bundesverfassungsgerichts wurde das „Recht auf Informationelle Selbstbestimmung“ als Grundrecht anerkannt. Das Bundesverfassungsgericht erklärte die damals bevorstehende Volkszählung als unzulässig, da sie nicht mit den Grundrechten der Menschenwürde und der allgemeinen Handlungsfreiheit vereinbar wäre:

„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag,
kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.“ [VZU]

So gewährt das Recht dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Es erlaubt jedem Individuum, selbst festzulegen, welche personenbezogenen Daten es preisgibt und wie diese Daten verwendet werden sollen. Um die Individualität einer Person zu schützen, gibt es weitere Gesetze in Deutschland, die unter anderem die Grundrechte der Meinungsfreiheit und Glaubensfreiheit gewährleisten sollen.

Für den Schutz der Informationellen Selbstbestimmung, die insbesondere in dem Bereich der Verarbeitung von personenbezogenen Daten mittels Informationstechnologien stark beeinflusst werden kann, wurden das Bundesdatenschutzgesetz und die Datenschutzgesetze der Bundesländer erlassen.

Das *Bundesdatenschutzgesetz* [BDSG] trat 1978 in Kraft und wurde 2001 an die Datenschutzrichtlinie der Europäischen Gemeinschaft angepasst. Bundesbehörden und Privatunternehmen sind zur Einhaltung dieses Gesetzes verpflichtet.
Im Bundesdatenschutzgesetz ist die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten prinzipiell verboten, außer eine klare Rechtsgrundlage erlaubt die Verarbeitung solcher Daten in einem konkreten Fall, oder die davon betroffene Person stimmt einer Nutzung ihrer Daten zu. Es gewährleistet weiterhin die in 95/46/EG enthaltenen Grundsätze der Datenvermeidung beziehungsweise Datensparsamkeit bei der Datenerhebung. Folglich dürfen nur so viele Daten, wie für einen bestimmten Zweck notwendig sind, gesammelt werden, um den Missbrauch dieser Daten einzugrenzen. Darüber hinaus soll auch von Verfahren wie der Anonymisierung und Pseudonymisierung von Daten Gebrauch gemacht werden. Um die Einhaltung dieser Bestimmungen zu prüfen, werden Datenschutzbeauftragte eingesetzt.

Für jedes deutsche Bundesland existieren nochmals eigene Landesdatenschutzgesetze. Diese regeln den Datenschutz in den öffentlichen Stellen des jeweiligen Bundeslandes. Private Firmen sind nicht durch diese Gesetze betroffen, müssen aber grundsätzlich das Bundesdatenschutzgesetz einhalten. Sowohl das Bundesdatenschutzgesetz als auch die Landesdatenschutzgesetze gelten nur, wenn für einen Sachverhalt kein bereichsspezifisches Spezialgesetz die Datenverarbeitung regelt. Spezialgesetze kommen zuerst zur Anwendung, da diese die höchste Priorität haben. Zu derartigen Spezialgesetzen gehören beispielsweise das Teledienstedatenschutzgesetz oder das Telekommunikationsgesetz.

In einem Gutachten von 2001 zur Modernisierung des deutschen Datenschutzes wurden die bestehenden Datenschutzregulierungen analysiert [Roß01a]. Dabei ist festgestellt worden, dass der Datenschutz in Deutschland sich an dem Stand der Informationstechnik der 70er Jahre orientiert. So ist der Einsatz von technikfernen Regelungen kritisiert worden, die die Vernetzung, Miniaturisierung, Leistungsfähigkeit, Ubiquität[1] und Mobilität der heutigen Zeit nicht ausreichend berücksichtigen. Des Weiteren wird darauf hingewiesen, dass die Datenverarbeitung größtenteils nicht transparent ist und sich insgesamt feststellen lässt, dass der deutsche Datenschutz überreguliert, zersplittert und unübersichtlich ist.

Zusätzlich zu den genannten Kritikpunkten lässt sich auch ein Vollzugsdefizit im Datenschutz erkennen. So wurde in einem Forschungsprojekt zum Thema „Scoringsysteme zur Beurteilung der Kreditwürdigkeit“ des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein herausgearbeitet, dass Verstöße gegen Datenschutzgesetze meist nicht erkannt und somit auch nicht verfolgt werden können [ULD06]. Gründe dafür werden darin gesehen, dass Personen, deren Daten unrechtmäßig verarbeitet werden, keine Kenntnis hiervon erhalten. Außerdem werden die staatlichen Datenschutzbehörden erst bei der Anzeige eines Verstoßes tätig und haben nicht die nötigen Ressourcen, alle Datenverarbeiter umfassend zu kontrollieren.

[1] bezieht sich auf *Ubiquitous Computing* und meint die Allgegenwärtigkeit der Technik.

3.3 Vergleich nationaler und internationaler Gesetze

Die internationalen Datenschutzgesetze und Richtlinien haben zwar den Schutz personenbezogener Daten und der Informationellen Selbstbestimmung zum Ziel, aber unterscheiden sich in ihren Umsetzungen. In einer Studie der *International Security, Trust and Privacy Alliance* (ISTPA) wurde 2007 verglichen, welche Gemeinsamkeiten es in den jeweiligen Datenschutzgesetzgebungen weltweit gibt [ISTPA]. Dabei wurden die einzelnen Gesetzgebungen gegenübergestellt und folgende Datenschutzerfordernisse identifiziert:

- *Accountability*: Zurechenbarkeit des Verantwortlichen für die Datenverarbeitung bei Verstößen gegen Regelungen und Gesetze.
- *Notice*: Informieren der betroffenen Person über Datenschutzpraktiken des Verantwortlichen und Aufklären über die Rechte der betroffenen Person.
- *Consent*: Zustimmung zur Datenverarbeitung durch die betroffene Person, Informieren über die Auswirkungen und über das Recht des Widerrufs.
- *Collection Limitation*: Zweckgebundene Datenerhebung, die sich auf das Erforderliche beschränken soll, um den vorgesehenen Zweck zu erfüllen.
- *Use Limitation*: Zweckgebundene Datenverarbeitung, so dass personenbezogene Daten nur verarbeitet werden, wenn dies dem ursprünglichen oder einem mit diesem zu vereinbarenden Zweck dient.
- *Disclosure*: Die Veröffentlichung, Übermittlung, Zugriffsbereitstellung, Verwendung für einen neuen Zweck und die Verbreitung von personenbezogenen Daten dürfen nur mit dem Wissen und der Zustimmung der betroffenen Person durchgeführt werden.
- *Access and Correction*: Zugang zu personenbezogenen Daten der jeweiligen Person und den Anspruch auf Korrektur bei falschen Inhalten.
- *Security Safeguards*: Sicherheitsmaßnahmen, die die Vertraulichkeit, Verfügbarkeit und Integrität personenbezogener Daten sicherstellen und kontrollieren.
- *Data Quality*: Stellt sicher, dass gesammelte Informationen dem Verwendungszweck gegenüber angemessen, relevant und nicht übermäßig sind. Außerdem sollen personenbezogene Daten genau und wenn erforderlich aktuell sein.
- *Enforcement*: Mechanismen, die die Einhaltung von Datenschutzrichtlinien sicherstellen und es ermöglichen, dass Individuen bei Verstößen Beschwerde einreichen können. Darüber hinaus müssen Verstöße entsprechend geahndet werden.
- *Openess*: Recht der betroffenen Person auf Einsicht der Datenschutzpraktiken des Datenverarbeiters.

Im Rahmen der genannten Studie ist dabei eine Übersicht entstanden (siehe Tabelle 3.1), die Einblick in die Datenschutzregelungen ausgewählter nationaler und internationaler Gesetze gewährt und offen legt, welche Datenschutzprinzipien in den einzelnen Gesetzen sichergestellt werden. In der genannten Tabelle werden beispielsweise die OECD Datenschutzrichtlinien, die Datenschutzrichtlinie der Europäischen Union und die Prinzipien von „Safe Harbor“ gegenübergestellt. Die rot hervorgehobenen Gesetze erfüllen die eben genannten Datenschutzprinzipien größtenteils umfassend und bieten von den verglichenen Gesetzen das höchste Maß an Datenschutz. Hierzu gehört auch die EU-Datenschutzrichtlinie.

	THE PRIVACY ACT OF 1974 (US)	OECD PRIVACY GUIDELINES	UN GUIDELINES CONCERNING COMPUTERIZED PERSONAL DATA	EU DATA PROTECTION DIRECTIVE	HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996	CANADIAN STANDARDS ASSOCIATION PRIVACY CODE	US FTC FAIR INFORMATION PRACTICES	SAFE HARBOR PRIVACY PRINCIPLES	AUSTRALIAN NATIONAL PRIVACY PRINCIPLES	JAPAN PERSONAL INFORMATION PROTECTION ACT	CALIFORNIA SB 1386, "SECURITY BREACH NOTIFICATION"	APEC PRIVACY FRAMEWORK
Accountability		X		X		X					X	X
Notice	X	X	X	X	X	X	X	X	X	X	X	X
Consent	X	X	X	X	X	X	X	X	X	X		X
Collection Limitation	X	X	X	X		X			X	X		X
Use Limitation	X	X	X	X	X	X		X	X	X		X
Disclosure	X				X	X		X	X	X		X
Access and Correction	X	X	X	X	X	X	X	X	X	X		X
Security/ Safeguards	X	X	X	X	X	X	X	X	X	X		X
Data Quality	X	X	X	X		X	X	X	X	X		X
Enforcement			X	X	X	X	X	X		X	X	X
Openness	X	X		X		X			X	X		X

Tabelle 3.1: Übersicht über die Gewährleistung von Datenschutzanforderungen in verschiedenen Gesetzgebungen der Welt (aus [ISTPA]).

3.4 Datenschutzgesetze in Bezug auf das eLearning

Durch die Vielzahl an Gesetzen, die zwar allgemein auf EU-Richtlinien basieren, aber auf Ebene der einzelnen Mitgliedsländern sehr verschieden umgesetzt werden, könnte sich die Realisierung eines datenschutzfreundlichen Lernmanagement-Systems sehr aufwendig gestalten.
Außerdem sind Lernmanagement-Systeme meist für kein konkretes Land konzipiert und somit ist die Einhaltung von länderbezogenen Gesetzen kaum durchführbar. Genauso gestaltet es sich mit der Unterscheidung der Gesetzgebung in öffentliche Behörden und Privatwirtschaft und die damit unterschiedlichen Anforderungen an den Datenschutz. So wird die Umsetzung von datenschutzfreundlichen eLearning- und Lernmanagement-Systemen durch den uneinheitlichen Datenschutz in den einzelnen Ländern erschwert. Außerdem ist bei multinationalen eLearning-Projekten unklar, welche Datenschutzgesetze Anwendung finden sollen.

Bei der Verwendung von eLearning-Programmen und insbesondere bei Lernmanagement-Systemen entstehen viele Informationen über die Benutzer, die als personenbezogene Informationen angesehen werden können. Nach Klobučar [Klo06] gehören zu personenbezogenen Informationen im eLearning die meisten in Lernprofilen enthaltenen Informationen. Dazu zählt Klobučar neben identifizierenden Informationen auch Suchaktivitäten von Lernenden, Login-Informationen und die IP-Adresse.

Ein weiterer Aspekt ist der wachsende Einsatz von *Ubiquitous Computing.* Denn, werden derartige Techniken für das vernetzte Lernen eingesetzt, ist es nicht mehr möglich, eindeutig festzustellen, wer personenbezogene Daten kontrolliert [PRI06]. Die Datenerfassung und Übermittlung ist für den Benutzer nicht mehr überschaubar und wer alles an einer Datenverarbeitung beteiligt ist, ist nicht ohne weiteres feststellbar. Somit gestaltet sich der Ausgangspunkt für den Datenschutz um einiges komplizierter.

Bei einer Auseinandersetzung mit Datenschutz und eLearning identifiziert Loser in [Los06] einen Konfliktbereich, der sich insbesondere auf die Hochschullehre bezieht. So ist es einerseits durch die Hochschulgesetze zum Zwecke der Lehre erlaubt, personenbezogene Informationen von Studierenden zu verarbeiten. Andererseits soll das Recht auf Informationelle Selbstbestimmung gewährt werden, welches durch die Datenschutzgesetze gewährleistet wird. Der genannte Konfliktbereich ist nochmals in Abbildung 3.1 visualisiert. Die methodische und inhaltliche Gestaltung der Lehre ist beispielsweise nach dem Hochschulgesetz Nordrhein-Westfalens durch den Lehrenden zu entscheiden. Weiter wird aber auch gefordert, dass die Treue zur Verfassung beizubehalten ist. So ist hier abzuwägen, welche Datenverarbeitungspraktiken nach den geltenden Gesetzgebungen für die Lehre erforderlich sind.

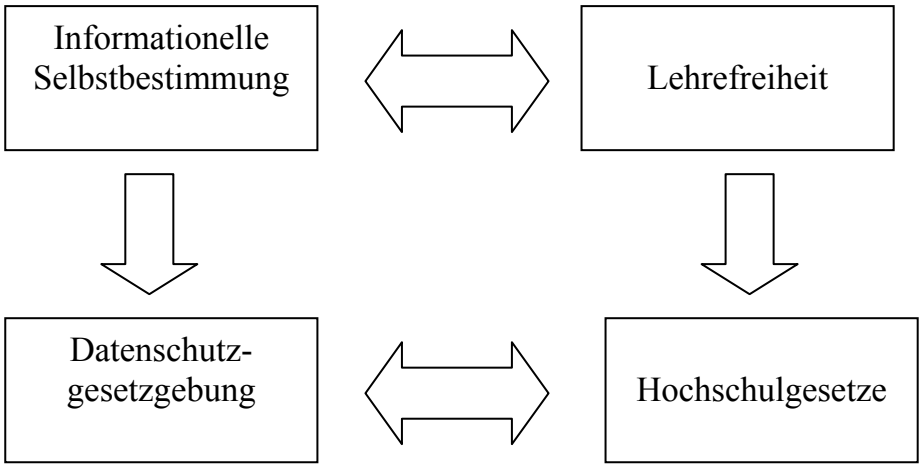

Abbildung 3.1: Konfliktbereich Datenschutz-Hochschule; aus [Los06]

3.5 Datenschutzgesetze in Bezug auf Minderjährige

Insbesondere im Bereich des (Schul-)Unterrichts, aber auch im eLearning ist die Frage zu klären, ob minderjährige Schüler wirksame Einwilligungen zur Datenverarbeitung geben können Die Veröffentlichung „Datenschutz in Schulen“ [Hes05], die sich mit den Datenschutzgesetzen für den Schulsektor auseinandersetzt, erläutert dabei die genannte Fragestellung bezogen auf das Hessische Datenschutzgesetz und das Hessische Schulgesetz. Darin

wird ausgesagt, dass die Datenverarbeitung von personenbezogenen Daten über gesundheitliche Beeinträchtigungen und die Datenverarbeitung für Forschungszwecke nur mit der Einwilligung der Erziehungsberechtigten vorgenommen werden darf. Im Übrigen gilt, dass minderjährige Schüler dann eine wirksame Einwilligung geben können, wenn sie die Tragweite der Entscheidung einschätzen können, ansonsten ist die Einwilligung der Erziehungsberechtigten einzuholen. Je jünger die Schüler sind, desto mehr Sorgfalt ist auf die Aufklärung der Schüler über Zweck und Umfang der Datenverarbeitung sowie das Auskunfts- und Widerspruchsrecht zu verwenden. Auch hier ist zu beachten, dass es für jedes Bundesland ein eigenes Schulgesetz beziehungsweise Hochschulgesetz gibt, das die Regulierung des Datenschutzes in Schulen und Hochschulen gestaltet.

Abschließend sollen nun noch beispielhaft Gesetze aufgeführt werden, die den Datenschutz bei Kindern und Schülern in den Vereinigten Staaten regulieren. So gibt es einerseits in den USA das *Family Educational Rights and Privacy Act* (FERPA), das die Grundlage zur Handhabung von Studenteninformationen und zum Schutz von Schüler- und Studenteninformationen ist. Andererseits soll mit dem *Children's Online Privacy Protection Act* (COPPA) außerdem die Privatsphäre von Kindern im Internet geschützt werden. Hier ist es Anbietern von Webseiten nur erlaubt, personenbezogene Daten über Kinder unter 13 Jahren zu sammeln, wenn die Eltern dem nachweisbar zustimmen.

3.6 Zusammenfassung

Die Hauptprinzipien des Datenschutzes und insbesondere des europäischen Datenschutzes setzen sich aus der Datenvermeidung bzw. –sparsamkeit, der Erforderlichkeit und Zweckbindung zusammen. Nach der Erhebung der Daten sind technische und organisatorische Maßnahmen zu treffen, um den Datenschutz zu gewährleisten und die Vertraulichkeit zu wahren. Ferner müssen die Bedingungen für die Rechtmäßigkeit der Datenverarbeitung eingehalten werden und die Rechte der betroffenen Personen sichergestellt werden. Des Weiteren ist die Datenverarbeitung soweit transparent zu gestalten, dass die betroffenen Personen ausreichend über die Verarbeitung ihrer Daten informiert werden. Nur eine transparente Datenverarbeitung bietet die Möglichkeit zur Wahrnehmung der Informationellen Selbstbestimmung eines Individuums.

Für die Einhaltung des Datenschutzes sind gegenwärtig die Datensicherheit durch Technik und die effektive Durchsetzbarkeit von Datenschutzanforderungen von großer Bedeutung. So setzt Datenschutz den Schutz vor unbefugter Einsichtnahme, Veränderung und Vernichtung voraus, was wiederum durch Techniken der Datensicherheit realisiert werden kann [Sch04]. Wann ein Sicherheitskonzept zum Schutz von personenbezogenen Daten angemessen ist, muss auf Grundlage einer Risikoanalyse festgestellt werden. Dabei muss auch der aktuelle Technikstand einbezogen werden. Als weitere Maßnahmen zum Datenschutz ist der Einsatz von datenschutzfreundlichen Technologien und eine datensparsame Gestaltung der Verarbeitung anzusehen. Außerdem wird in [Roß01b] vorgeschlagen, eine Zertifizierung von datenschutzfreundlichen Produkten vorzunehmen. Auf diese Weise könnte auch der Verbraucher datenschutzfreundliche Produkte erkennen und bei Bedarf diese den weniger datenschutzfreundlichen vorziehen.

Datenschutz und Informationelle Selbstbestimmung sind Rechte, die auf viele gegenläufige Interessen stoßen. Dabei konkurrieren diese Interessen miteinander oder widersprechen sich teilweise. So unterstützt Datenschutz die Rechte und Interessen des Individuums gegenüber der Gesellschaft. Der Datenschutz ist für die freie Entfaltung der Individuen von großer Be-

deutung. Aber auch die Gesellschaft hat Interessen, die durch den Datenschutz beeinträchtigt werden, wie z.B. die Aufdeckung von kriminellen Verhalten. Deshalb ist ein Ausgleich zwischen dem Schutz personenbezogener Daten des Einzelnen und Interessen staatlicher und privater Datenverarbeiter zu schaffen. Es sollte in jeder Situation, in der der Datenschutz andere Interessen beeinflusst, abgewogen werden, in welchen Maß der Schutz von personenbezogenen Daten gewährt werden sollte.

Organisationen und Einrichtungen, die personenbezogene Daten verarbeiten, sind daran interessiert, zu Personen, von denen sie sensible Daten sammeln, ein Vertrauensverhältnis aufzubauen. Aber auch für die weitreichende Akzeptanz des eCommerce und der elektronischen Kommunikation ist Vertrauen in die Anbieter notwendig. Bei den meisten Online-Angeboten bestehen jedoch bei der Angabe von personenbezogenen Daten nur zwei Möglichkeiten: diese anzugeben und der Datenverarbeitung zuzustimmen, um das Angebot zu nutzen, oder diese nicht anzugeben und demzufolge das Angebot nicht nutzen zu können.

4. Methodik der Datenschutzbewertung

Die Anforderungen, die es in den internationalen und nationalen Gesetzen zum Schutz der Informationellen Selbstbestimmung und des Datenschutz gibt, wurden in Kapitel 3 besprochen. Nun soll ein Evaluationsvorgehen erarbeitet werden, das eine Bewertung des Datenschutzes in Lernmanagement-Systemen ermöglicht.
In diesem Kapitel wird auf Bewertungsverfahren zur Evaluation von Lernmanagement-Systemen eingegangen und das methodische Vorgehen für die durchzuführende Datenschutzbewertung von Lernmanagement-Systemen festgelegt.

Zur Bewertung von Lernmanagement-Systemen werden in der Literatur zahlreiche Methoden vorgeschlagen. Im Folgenden werden ausgewählte Methoden vorgestellt, die nach Baumgartner et al. [Bau02] eine Bewertung und Auswahl von Lernmanagement-Systemen ermöglichen. Dazu gehören die Rezessionen, die Vergleichsgruppen, das Expertenurteil und die Kriterienkataloge. Der Fokus dieser Verfahren liegt neben der eigentlichen Bewertung meist darauf, eine Auswahl zu treffen, welches Lernmanagement-System die jeweiligen Bedingungen und Wünsche der Bewertenden am besten erfüllt und für den zukünftigen praktischen Einsatz an einer Institution am geeignetsten ist. Durch die Verfahren können aus der großen Menge vorhandener Systeme diejenigen ausgewählt werden, die bestimmten Anforderungen genügen.

4.1 Rezessionen

Bei Bewertungen auf Grundlage von Rezessionen wird auf Artikel oder Veröffentlichungen zurückgegriffen, die die zu bewertenden Produkte beschreiben aber auch bewerten können. Dabei steht weder die Vollständigkeit noch die Objektivität der Betrachtung im Vordergrund. Es sollen vielmehr subjektive Erfahrungen und Einschätzungen für die eigene Bewertung oder Auswahl hinzugezogen werden.
Das Fokussieren auf externe Berichte hat dabei die Vorteile, dass dies sowohl kostengünstig ist als auch meist keinen größeren Arbeitsaufwand bedeutet. Als nachteilig ist aber die nicht einheitliche Gestaltung dieser Artikel zu nennen, die kaum Gegenüberstellungen von Produktbeurteilungen zulassen. Da es sich um subjektive Betrachtungen der Ersteller handelt, ist mittels einer Rezession kaum eine objektive Sichtweise auf ein Lernmanagement-System durch Außenstehende möglich.

4.2 Vergleichsgruppen

Eine Bewertung von Lernmanagement-Systemen kann auch mit Hilfe einer Beobachtung mehrerer Gruppen von Lernenden durchgeführt werden. Diese Gruppen müssen in ihrer Zusammensetzung vergleichbar sein. Sie bearbeiten jeweils mit einem anderen Lernmanagement-System eine festgelegte Aufgabe. Dadurch können Differenzen, die bei der Anwendung der zu bewertenden Lernplattformen auftreten, ermittelt werden.
Durch die Verwendung von Vergleichsgruppen ist eine objektive und nach wissenschaftlichen Standards durchgeführte Untersuchung möglich. Andererseits ist der Aufwand der Erhebung und Auswertung relativ hoch im Vergleich zu anderen Bewertungsverfahren. Trotz des wissenschaftlichen Vorgehens kann es zu Schwierigkeiten bei der Isolierung von einzelnen Faktoren kommen, auf denen die Schlussfolgerungen für die Gebrauchstauglichkeit und

Lernunterstützung der Lernplattform basiert. So ist beispielsweise nicht nur das Anpassen von Lernstoff an die jeweilige Lernplattform für deren Interaktivität ausschlaggebend, sondern auch ob der Lernstoff mit allen zur Verfügung stehenden Mitteln präsentiert wird.

4.3 Expertenurteil

Bei diesem Bewertungsverfahren stellen Experten in Gruppensitzungen Kriterien und Maßstäbe auf, auf denen die jeweilige Untersuchung aufbaut. Dabei ergeben sich meist Resultate, die die Vorstellungen der Expertengruppe widerspiegeln und stark situationsbedingt sind. Folglich müssen diese Ergebnisse nicht unbedingt nachvollziehbar sein und auch die Reproduzierbarkeit ist bei diesem Verfahren nicht gegeben. So kommen unterschiedliche Expertengruppen zu unterschiedlichen Ergebnissen, aber auch bei einer einzelnen Gruppe ist nicht gewährleistet, dass dieselben Kriterienschwerpunkte zweimal ermittelt werden. Die einzelnen Ansichten sind dabei vor allem bei der Aufstellung von Kriterien von Bedeutung.
Eine Bewertung von Lernmanagement-Systemen anhand von Experten bietet hingegen zuverlässige Ergebnisse. Dabei reichen schon relativ wenige Experten aus, um eine umfassende Aufstellung von Ergebnissen zu erhalten [Mer]. So können wenige Experten genügen, um ein Lernmanagement-System aussagekräftig zu evaluieren.

4.4 Kriterienkataloge

Ein Kriterienkatalog ist eine Bewertungsmethode, die bei Evaluationen von Lernmanagement-Systemen sehr häufig zum Einsatz kommt. So wurde diese Herangehensweise beispielsweise auch in den Untersuchungen von Baumgartner et al. [Bau02] und Schulmeister [Sch05] als Hauptmethode zur Bewertung angewandt. Außerdem wurden in 23 weiteren internationalen Studien ebenfalls Kriterien zur Beurteilung von Lernmanagement-Systemen verwendet [Sch05].

In Form von Prüf- oder Checklisten werden bei diesem Verfahren die Qualität und der funktionale Umfang von Produkten bewertet. Es werden Kriterien formuliert, die in einer Checkliste oder einem Fragebogen abgearbeitet werden. Diese Kriterien können durch Hersteller, Anbieter, Anwender oder Begutachter von Lernmanagement-Systemen ausgefüllt werden. Dabei ist es möglich, neben einer Angabe, ob ein Kriterium überhaupt vorhanden ist, auch zu beurteilen, in welchem Maß dieses Kriterium erfüllt, beziehungsweise wie gut es in der Lernplattform realisiert wird. Außerdem hat man die Möglichkeit, Kriterien zu gewichten. Dadurch kann der Fokus auf Eigenschaften gesetzt werden, die bei der Untersuchung als besonders relevant eingestuft werden. Durch eine Gewichtung der Kriterien kann eine Filterung nach bestimmten Anforderungen ermöglicht werden. Dabei kann auch eine Rangordnung entstehen, bei der die Produkte, die die Kriterien am besten erfüllen, weiteren Untersuchungen unterzogen werden, während Produkte, die die Kriterien nicht oder kaum erfüllen, vorzeitig ausgeschlossen werden. Auf diese Weise kann eine wesentliche Effizienzsteigerung der Untersuchung erreicht werden.

Das Verfahren der kriterienorientierten Bewertung hat jedoch auch Nachteile. So ist ein Nachteil einer als Befragung durchgeführten kriterienorientierten Evaluation, dass sie von der Korrektheit der Angaben des jeweilig Beantwortenden abhängig ist. Des Weiteren kann eine allumfassende Betrachtung des Produktes durch diese Methode nicht gewährleistet werden. Es können sich Kriterien ergeben, die für die jeweilige Interessengruppe von großer Relevanz sind und dadurch in viele Unterkategorien aufgespaltet werden. Andere Kriterien sind hinge-

gen ohne Bedeutung für die Untersuchung und werden eventuell nicht als Kriterium einbezogen. Bei der Anwendung von Gewichtungs- bzw. Bewertungsverfahren können die verwendeten Faktoren subjektiv gewählt oder für ein konkretes Anwendungsszenario bestimmt sein. So können aus den Ergebnissen von objektiven Kriterienkatalogen durch eine Vielzahl von möglichen Gewichtungen sehr subjektive Entscheidungen resultieren, die nicht immer nachvollziehbar sind. Folglich kann die umfassende und objektive Bewertung nicht mehr gewährleistet werden. Es existiert beispielsweise auch nach Baumgartner kein allgemein akzeptiertes Gewichtungsverfahren für Kriterien von Lernmanagement-Systemen.
Darüber hinaus beinhaltet das Vorhandensein einer Funktion noch keine Aussage über die Qualität dieser. Die Umsetzung einer Funktion in zwei verschiedenen Lernmanagement-Systemen kann aber sehr unterschiedlich realisiert sein. Wodurch beispielsweise die Gebrauchstauglichkeit dieser Funktion variieren kann.

Als Vorteile gegenüber den anderen Bewertungsverfahren werden die Kostengünstigkeit, die einfache Organisation und das methodische Vorgehen angesehen. So kann eine fachkundige Person genügen, die die Lernplattform testet und die Liste der festgelegten Kriterien abarbeitet. Es muss keine Testumgebung geschaffen werden, in der das Lernmanagement-System erprobt wird. Des Weiteren bleiben durch die einheitliche Betrachtung mittels Kriterienkatalog die Ergebnisse vergleichbar, die auf dem selben Kriterienkatalog beruhen.

4.5 Geplante Durchführung der Bewertung

Ein optimales Bewertungsverfahren gibt es nach Aussage von Autoren wie Baumgartner nicht. Die verschiedenen Verfahren haben Vor- und Nachteile, die es bei der Betrachtung zu berücksichtigen gilt. Das Expertenurteil ist vornehmlich zur Erarbeitung von Kriterien für einen bestimmten Anwendungsbereich gedacht. Dies wäre in der hier durchzuführenden Untersuchung angebracht, falls konkrete Datenschutzbestimmungen auf ein Lernmanagement-System abgebildet werden müssten und die Ideen zur Umsetzung durch beteiligte Experten geliefert werden sollen. Für eine Untersuchung der allgemeinen Datenschutzfreundlichkeit ist dies aber nicht zweckmäßig. Ähnlich verhält es sich mit den Vergleichsgruppen. Deren primäres Ziel ist die Unterstützung des Lernens, Lehrens und der Gebrauchstauglichkeit festzustellen. Dies ist zwar für die Untersuchung der Umsetzung von datenschutzfreundlichen Funktionen wichtig, aber für die Bewertung der Datenschutzunterstützung allgemein für diese Arbeit nicht relevant.

Betrachtet man die Literatur eingehender, so fällt auf, dass die meisten Untersuchungen auf einer kriterienorientierten Evaluation durch Befragung basieren.
Aufgrund der guten Vergleichbarkeit von Angaben, die durch die Verwendung eines Kriterienkataloges entstehen, erscheint dieses Verfahren auch für die hier durchzuführende Untersuchung als geeignet. Dabei sollte der Kriterienkatalog von fachkundigen Personen wie zum Beispiel Anbietern oder Administratoren ausgefüllt werden, die auch mit den datenschutzrelevanten Funktionen und Einstellungen des jeweiligen Systems vertraut sind.

Für eine Datenschutzuntersuchung von Lernmanagement-Systemen ist außerdem zu beachten, dass der Datenschutz an sich kein explizit kapselbares Feature einer Software ist, sondern an vielen Stellen eines Systems zum Einsatz kommen kann und somit Datenschutzelemente mit der gesamten Anwendung verwoben sind.

Aus diesem Grund sollen – sofern möglich – durch persönliches Testen der Lernumgebungen die Umsetzung einzelner Datenschutzkriterien untersucht werden und weitere implizit vor-

handene Informationen zur Handhabung von datenschutzrelevanten Funktionen gesammelt werden. Um die Untersuchung abzurunden, ist überdies geplant, Erfahrungen anderer Quellen mit den einzelnen Lernmanagement-Systemen in Form von Rezessionen und anderen Veröffentlichungen hinzuzuziehen.

5. Die Bewertungskriterien

In diesem Kapitel werden zuerst Veröffentlichungen vorgestellt, die zur Gewinnung eigener Bewertungskriterien dienen sollen. Dabei werden einerseits Bewertungskriterien für Software-Produkte und andererseits für eLearning-Systeme sowie für Lernmanagement-Systeme betrachtet, die die Sicherheit und den Datenschutz fokussieren. Diese sollen im weiteren Verlauf der Arbeit neben den in Kapitel 3 behandelten Gesetzen als Grundlage für eigene Bewertungskriterien dienen. Im Anschluss daran werden im zweiten Abschnitt des Kapitels die eigenen Bewertungskriterien eingehend dargestellt. Abgeschlossen wird die Erarbeitung der Kriterien für die Datenschutzbewertung von Lernmanagement-Systemen mit einer zusammenfassenden Betrachtung.

5.1 Recherche von Kriterien für eine Datenschutzbewertung

Um geeignete Kriterien für die Datenschutzbewertung zu formulieren, werden in diesem Abschnitt Studien, Veröffentlichungen und andere Quellen betrachtet, die sich mit der Bewertung von Datenschutz- und Sicherheitsmaßnahmen beschäftigen. Es wird ein Einblick in die Bewertungsvorgehen aus angrenzenden Bereichen der Software- und eLearning-Systeme gegeben. Dabei beruhen die Analyse des Datenschutzes und das Definieren von diesbezüglichen Anforderungen meist auf Datenschutzrichtlinien und –Gesetzen.

5.1.1 Bewertungskriterien für Softwareprodukte

Für einen Einblick in Verfahren, die den Datenschutz von Software-Produkten bewerten, soll im Folgenden ein Vorgehen bei der Vergabe von Datenschutzgütesiegeln vorgestellt werden.

Unter Leitung des unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) wurde im Juni 2007 mit dem Projekt „European Privacy Seal“ (kurz EuroPriSe) begonnen. Im Rahmen von EuroPriSe werden Anforderungen für ein europäisches Datenschutzsiegel erarbeitet, das die Einhaltung von Datenschutz- und IT-Sicherheitsbestimmungen widerspiegelt [ULD07]. Dabei ist es im Interesse der Europäischen Kommission, die dieses Projekt fördert, ein für den europäischen Raum gültiges Gütesiegel zu etablieren und eine Zertifizierung von datenschutzkonformer Software zu unterstützen. Das Projekt baut auf den Erfahrungen bei der Realisierung des Gütesiegel-Verfahrens für Schleswig-Holstein auf. Da das Projekt erst begonnen wurde und noch keine Resultate über den Aufbau und den Inhalt vorliegen, wird im Folgenden stellvertretend die Vorgehensweise des Vorgängerprojektes „Gütesiegel Schleswig-Holstein“ eingehender betrachtet.

Das unabhängige Landeszentrum für Datenschutz Schleswig-Holstein hat für die Begutachtung von Software-Produkten hinsichtlich deren datenschutzgerechter Umsetzung ein Verfahren entwickelt, dass es erlaubt, Programme, die bestimmten Anforderungen entsprechen, nach eingehender Analyse ein Gütesiegel zuzusprechen. So werden insbesondere Software-Systeme, die der behördlichen und gesundheitsmedizinischen Verwaltung und Verarbeitung von personenbezogenen Daten dienen, auf ihre Datenschutzunterstützung geprüft. Dafür bewerten Sachverständige des Datenschutzes beziehungsweise Datenschutzbeauftragte die Software unter verschiedenen Gesichtspunkten. Um die Bewertung solcher Programme zu vereinheitlichen, wurde im Rahmen des Gütesiegel-Verfahrens ein Anforderungskatalog zusammengestellt.

Da das ULD hauptsächlich auf Länderebene für das Bundesland Schleswig-Holstein zuständig ist, ist dieses Verfahren auf die Datenschutzgesetzgebung dieses Bundeslandes ausgelegt. Das Gütesiegelverfahren stützt sich damit hauptsächlich auf das Landesdatenschutzgesetz (LDSG) in Verbindung mit der Datenschutzverordnung (DSVO) Schleswig-Holsteins. Ferner werden je nach beabsichtigter Einsatzart weitere Gesetze, wie beispielsweise das Bundesdatenschutzgesetz (BDSG), das Sozialgesetzbuch (SGB) und das Teledienstedatenschutzgesetz (TDDSG) berücksichtigt. Datenschutz-Beauftragte aus anderen Bundesländern wie zum Beispiel Mecklenburg-Vorpommern, Brandenburg, Nordrhein-Westfalen und Brandenburg empfehlen aber den dort ansässigen Behörden ebenfalls Software einzusetzen, die durch das Gütesiegel des ULD zertifiziert wurde [ULDFAQ]. Datenschutzgesetze der einzelnen Länder können, wie schon in Kapitel 3 beschrieben, von Bundesland zu Bundesland abweichen, basieren aber alle auf den Datenschutzrichtlinien der Europäischen Gemeinschaft.

Im Weiteren soll der Anforderungskatalog [ULD05], der als Leitfaden für das Gütesiegel-Verfahren Schleswig-Holstein dient, betrachtet werden. Er ist inhaltlich in vier Komplexe unterteilt. Die folgenden Ausführungen stellen nur einen Überblick über die im Anforderungskatalog vorkommenden Fragestellungen dar. Eine ausführliche Übersicht befindet sich in Anhang A.

Der erste Komplex beschäftigt sich mit der Gestaltung der Technik und prüft insbesondere die Anforderungen der Datenvermeidung und Transparenz. Darin enthalten sind Fragestellungen, die überprüfen, ob eine anonyme oder auch pseudonyme Nutzung des IT-Produktes durch den Betroffenen möglich ist, ob und welche personenbezogenen Daten wirklich erforderlich sind und wann diese Erforderlichkeit endet und somit die Daten zu löschen sind. Des Weiteren wird in diesem Komplex überprüft, in welchem Maß die Datenflüsse, Speicherorte, Übermittlungswege und Zugriffsmöglichkeiten für die Anwender und Administratoren, aber auch für die Betroffenen transparent gestaltet sind. Hierbei wird auch die Produktbeschreibung hinzugezogen und deren Verständlichkeit und umfassende Konzepterläuterung kontrolliert.

Der zweite Komplex soll auf Grundlage von Datenschutzbestimmungen überprüfen, ob die angestrebte Datenverarbeitung zulässig ist. Dabei ist zunächst - je nach vorgesehener Einsatzstelle - zu prüfen, welches Recht anzuwenden ist.
Ist dies geklärt, kann die Rechtmäßigkeit der Datenverarbeitung überprüft werden. So kann entweder eine Ermächtigung durch das Gesetz vorliegen oder es muss die Einwilligung jedes Betroffenen eingeholt werden. Hierbei kann das IT-Produkt eine Mustererklärung zur Einwilligung zur Verfügung stellen oder es unterstützt den Anbieter zumindest bei der Erstellung dieser. Es ist zu überprüfen, ob die Einwilligungserklärung vor der ersten Speicherung von personenbezogenen Informationen durch das Programm angeboten wird. Eine Vorraussetzung, um die Rechtmäßigkeit der Datenverarbeitung im Nachhinein zu überprüfen, ist eine geeignete Protokollierung der Datenverarbeitung. Dadurch kann auch die Einhaltung der Zweckbindung überwacht werden.

Eine Überprüfung der technisch-organisatorischen Maßnahmen, die ein IT-Produkt zum Schutz von personenbezogenen Daten anbietet beziehungsweise unterstützt, findet im dritten Komplex statt. Es wird überprüft, welche Verfahren zur Vermeidung unbefugten Zugangs, unbefugter Einsicht und unbefugter Weiterverarbeitung verwendet werden. Authentifizierung und die Vergabe von Zugriffsrechten an autorisierte Personen können zur Realisierung der Anforderungen aus diesem Komplex eingesetzt werden. Weiterhin sind hier Firewall- Software und Verschlüsselungsverfahren als unterstützende Maßnahmen zu nennen. Aber auch die verständliche Darstellung der Datenverarbeitung einer Software durch entsprechende Hinweise und Informationen steigert die Sensibilität der Anwender, die mit personenbezoge-

nen Daten arbeiten, und trägt somit zur Vermeidung unbeabsichtigter Datenschutzverletzungen bei. Ein wichtiger Faktor ist hier auch eine ausreichende Gewährleistung der Verfügbarkeit, Integrität und Vertraulichkeit.
Bei der Beurteilung von Software-Systemen ist in diesem Komplex weiterhin zu klären, welche Angreifermodelle zugrunde liegen, welche Schutzmaßnahmen dagegen vorgesehen sind oder noch fehlen und welche Restrisiken zurückbleiben.

Der vierte Komplex beinhaltet Kriterien um die Realisierung der Rechte, die Betroffene in Anspruch nehmen können, zu beurteilen. Dafür muss das Konzept der Software für den Betroffenen transparent gestaltet werden, um diesen über den Rahmen der Datenverarbeitung aufzuklären. Auch sollte die Software bei einem Einwand beziehungsweise Widerspruch des Betroffenen, die dafür benötigten Vorgänge unterstützen. Hier ist von Relevanz, ob und wie die Wahrnehmung dieser Rechte gefördert werden und ob eine technische Unterstützung zur Gewährleistung dieser Rechte gegeben ist.

Die vier vorgestellten Komplexe fließen in die abschließende Beurteilung unter Berücksichtigung von deren Relevanz, Aufwand, Stand der Technik, Konfigurationsmöglichkeiten und Dokumentation in gleicher Gewichtung ein. Abschließend wird allgemein beurteilt, ob die Software zur Erfüllung von Datenschutzanforderungen beiträgt, diese erschwert oder den Datenschutz nicht beeinflusst. Die Komplexe werden einmal für personenbezogene Daten, welche die Primärdaten darstellen wie auch für die bei der Verwendung des IT-Produktes entstehenden Protokollierungsdaten betrachtet.

Im Falle von Lernmanagement-Systemen sind die Benutzer der Software und die Betroffen der Datenverarbeitung dieselbe Personengruppe. In anderen Fällen verarbeitet Software meist persönliche Informationen von Betroffenen, ohne dass sie die Möglichkeit erhalten, diese Software auch zu benutzen.

5.1.2 Bewertungskriterien für eLearning-Systeme

5.1.2.1 Datenschutzkriterien im universitären Umfeld

Das White Paper von CAUSE [CAU97], welches hier näher betrachtet werden soll, beschäftigt sich mit dem speziellen Umfeld des Datenschutzes an Universitäten und Kollegs in den USA. Da dabei insbesondere auf die elektronisch-vernetzte Infrastruktur an diesen Einrichtungen eingegangen wird, soll es zur Betrachtung von eLearning-Systemen und deren Datenschutzbewertung hinzugezogen werden. Als Grundlage der Veröffentlichung nutzt CAUSE den *Family Educational Rights and Privacy Act* (FERPA) von 1974. Wie schon in Kapitel 3 erläutert, reguliert FERPA den Datenschutz bezüglich Bildungsinformationen von Schülern. Das Gesetz wird seit 1974 angewendet und es bezieht dadurch weder moderne Techniken noch deren Folgen für die Datenverarbeitung mit ein. Seit damals wurden keine neuen Regelungen auf dem Gebiet in den USA verabschiedet. Die Veröffentlichung von CAUSE zeigt aber auf, welche Faktoren nach dem Stand der modernen Technik neu betrachtet werden müssten, wo Veränderungen von Nöten wären und welche Aspekte unter den gegebenen Umständen neu hinzukommen sollten. So hat CAUSE den Fokus speziell auf die Evaluation von Informationstechnologien hinsichtlich des Datenschutzes von Studenteninformationen gerichtet. In dem White Paper werden Fragestellungen angeführt, die es zu klären gilt, um den Datenschutz an Universitäten adäquat umzusetzen. Zur angemessenen Handhabung von personenbezogenen Informationen werden in der Untersuchung folgende Prinzipien vorgestellt, die es zur Erfüllung des Datenschutzes zu realisieren gilt:

- Notification,
- Minimization,
- Secondary Use,
- Nondisclosure and Consent,
- Need to Know,
- Data Accuracy, Inspection, and Review,
- Information Security, Integrity, and Accountability,
- Education.

Diese acht von CAUSE ermittelten Kriterien für die Einhaltung des Datenschutzes werden nun eingehend erläutert. Dabei wird auf Faktoren und Fragestellungen eingegangen, die bei einer Realisierung der Kriterien zu betrachten sind.

Notification: Dieses Kriterium beinhaltet die Aufklärung der Studierenden über die Verarbeitung von Informationen, die durch und über sie gesammelt werden. Hier ist zu überlegen, wie häufig, mit welcher Intensität und in welchem Umfang diese Aufklärung vorgenommen werden sollte.

Minimization: Es wird bei diesem Kriterium eine datensparsame Datenverarbeitung, die sich nur auf das Erforderlichste bezieht, angestrebt. Dabei werden die Datenarten und die Menge der Daten betrachtet, die von und über Studenten erhoben werden. Trotz einer datensparsamen Datenerhebung soll noch der Zweck der Datenverarbeitung erreicht werden können. Außerdem sollte in die Betrachtung mit einbezogen werden, wann Daten nach Wegfall der Erforderlichkeit zu löschen sind beziehungsweise wie archivierte Datenbestände zu handhaben sind. Faktoren, wie die verteilte Datenhaltung, die Quelle, von der die personenbezogenen Daten zur Verfügung gestellt werden, und die Sensitivität der einzelnen personenbezogenen Daten sollten weiterhin in die Betrachtung einbezogen werden, um den Anspruch der Datenminimierung zu unterstützen. Darüber hinaus sollte auch die Datenerhebung für den Zweck der Sicherheitsüberwachung oder für Notsituationen hier nicht vernachlässigt werden. Beispielsweise sollte abgewogen werden, ob und in welchem Ausmaß die Sicherheit eines Institutes wichtiger ist als der Schutz der Privatsphäre der Studenten.

Secondary Use: Informationen über Studenten sollen für dieses Kriterium nur für den Zweck, für den sie erhoben wurden, von den selben Instituten verarbeitet werden, beziehungsweise für Zwecke, die mit dem ursprünglichen Zweck vereinbar sind. Der Zweck der Datenverarbeitung sollte nur mit der Zustimmung der betroffenen Person geändert werden, weshalb dieses Kriterium eng mit denen der *Notification*, *Minimization*, *Nondisclosure and Consent* verbunden ist. Als Vorraussetzung für dieses Kriterium, muss zum Zeitpunkt der Datenerhebung der Zweck präzise angegeben werden. Nur dann kann man sich in späteren Phasen daran orientieren.

Nondisclosure and Consent: Zur Erfüllung dieses Kriteriums dürfen personenbezogene Daten der Studenten nicht an Dritte außerhalb der Universität weitergegeben werden. Es sei denn die betroffenen Studenten haben dem zugestimmt. Dabei gibt es zwei Methoden, wie ein Student sein Einverständnis ausdrücken kann. Bei der „opt-out"-Methode werden personenbezogene Informationen nach Benachrichtigung der Studenten weitergegeben. Dieser Datenverarbeitung kann ein Student widersprechen. Nimmt er dieses Recht nicht wahr, stimmt er der Weitergabe implizit zu. Im Gegensatz dazu werden personenbezogene Informationen der Studenten bei der „opt-in"-Methode solange vertraulich behandelt und nicht an Dritte weitergegeben, bis der Student eine schriftliche Erlaubnis zur Weitergabe erteilt. Die zweite Metho-

de wird meist bei als sehr sensibel eingestuften Informationen verwendet. Die Einstufung der Sensibilität von personenbezogenen Daten wird laut CAUSE von jedem Institut eigenständig festgelegt. Dabei hält es CAUSE für angebracht, den einzelnen Studenten mit entscheiden zu lassen, wie seine Daten einzustufen sind, da jede Person hier verschiedenartige Ansichten haben kann. So wird vorgeschlagen, dass ein Student bestimmte Angaben über sich beispielsweise in eine geschütztere Kategorie als bisher einordnen kann. Dies kann zum Beispiel mittels flexibler, technischer Verfahren, Maßnahmen und Systemen geschehen. Jedoch ist zu überlegen, wie viel Einfluss ein Student auf die Datenverarbeitung haben sollte.

Need to Know: Für die Erfüllung diese Prinzips soll nur Personen der Zugriff auf personenbezogene Daten von Studenten gewährt werden, die legitime Ausbildungsinteressen haben und laut der Datenschutzvereinbarung dazu ermächtigt sind. Dieses Prinzip ist an berufliche Aufgaben, den Zweck und den Umfang der geplanten Verwendung von personenbezogenen Informationen geknüpft. Wem welche Tätigkeiten als legitime Bildungsinteressen zugeschrieben werden, kann laut CAUSE jede Hochschule eigenständig festlegen. Software-Systeme, die im Hochschulbereich eingesetzt werden, sind nicht zwingend konform mit den Rechten, die an einer Hochschule definiert sind, da sie keine beziehungsweise eigene Zugriffsrechte für die jeweiligen Rollen festlegen. Außerdem sollte vermieden werden, dass Software-Systeme Informationen gemeinsam darstellen, für die unterschiedliche Befugnisse vergeben wurden. Ansonsten könnte es passieren, dass bei der Einsicht in personenbezogene Information gleichzeitig weitere Informationen sichtbar sind, für die die Person keine Zugriffsrechte hat. Folglich sollte überprüft werden, ob ein IT-Produkt so gestaltet ist, dass es mit den Datenschutzregeln eines Institutes in Einklang gebracht werden kann.

Data Accuracy, Inspection, and Review: Dieses Prinzip beinhaltet, dass personenbezogene Daten, die durch ein Institut erhoben werden, korrekt sein sollten. Außerdem soll den Studenten ermöglicht werden, Einsicht in ihre personenbezogenen Daten zu nehmen sowie Änderungen dieser Daten zu veranlassen, falls diese nicht korrekt sind. In einer verteilten Umgebung kann die Einsicht auf die eigenen personenbezogenen Daten vereinfacht werden, da es nicht mehr notwendig ist, alle Verwaltungsstellen aufzusuchen, die entsprechende Daten gespeichert haben.
Zusätzlich ist zu beachten, dass bei der Interaktion mit Serviceautomaten oder Computern Transaktionsdaten entstehen, die Auskünfte über das Verhalten eines Studenten geben können und somit als personenbezogene Daten betrachtet werden können. Solche Transaktionsdaten können beim Bezahlen von Mahlzeiten, Ausleihen von Büchern oder Benutzen von Computern entstehen. Dabei ist zu überlegen, in welchem Ausmaß diese Daten den Studenten für Einsichtnahme und Überprüfung zugänglich sein sollten.

Information Security, Integrity, and Accountability: Die Unterstützung der Sicherheit, Integrität und Zurechenbarkeit von Daten in Software-Systemen, wird bei diesem Prinzip betrachtet. Zur Einhaltung des Prinzips müssen personenbezogene Daten vor Verlust, unsachgemäßem Zugang, unerlaubter Preisgabe und Modifikation geschützt werden. Bei sicherheitsrelevanten Ereignissen ist außerdem zu klären, wem bestimmte Aktionen zuzuordnen sind.
Maßnahmen, um dieses Prinzip sicherzustellen, sollten unter Einbeziehung der Schutzwürdigkeit der jeweiligen Informationen und der Bewertung des allgemeinen Risikos gewählt werden. In der Studie von CAUSE wird explizit darauf hingewiesen, dass auch Aktivitätsdaten und System-Logs über Studenten zu schutzwürdigen Daten zählen und somit in die Betrachtung einbezogen werden sollten.
Die konkreten Sicherheitsmaßnahmen, die ergriffen werden, um personenbezogene Daten angemessen zu schützen, sind den jeweiligen Institut überlassen. Die Institute sind jedoch dazu verpflichtet, formale Sicherheitsregeln aufzustellen sowie Rollen und Verantwortlichkei-

ten zu vergeben, um Verletzungen der Sicherheit ausfindig zu machen und deren Ursprung zu ermitteln. In den von CAUSE untersuchten universitären Einrichtungen wurden folgende Grundmaßnahmen zur Gewährleistung der Sicherheit identifiziert: Gesicherte Übertragung, Authentifizierung, Autorisierung, physische Sicherheit der zentralen Komponenten sowie Protokollierung. Bezüglich der gesicherten Übertragung muss laut der Autoren im Einzelfall abgewogen werden, welche Verschlüsselungsverfahren und integritätssichernden Maßnahmen bei der Datenübertragung angebracht sind. Ein angemessenes Niveau der Protokollierung von Netzwerktransaktionen erlaubt eine detaillierte Darstellung von Ereignissen, die die Sicherheit gefährden können. Die gespeicherten Protokolldaten selbst stellen aber wiederum ein Risiko für die Privatheit dar. Deshalb ist zu überlegen, welche Informationen für eine Aufzeichnung notwendig und angebracht sind, damit auch das Prinzip der *Minimization* eingehalten werden kann.

Education: Dieses Prinzip fokussiert die Aufklärung, Weiterbildung beziehungsweise Sensibilisierung von Studenten, Administratoren und Mitgliedern von Instituten zum Thema Datenschutz. Inhaltlich sollen mögliche Auswirkungen der Verwendung und des Missbrauchs von personenbezogenen Daten aufgezeigt werden. Darüber hinaus soll der Einfluss der vernetzten Informations- und Kommunikationstechnik und die damit einhergehenden Bedenken für die Privatheit transparent gemacht werden. Derartige Aufklärungen sollten über die einfache Hinweispflicht hinausgehen. Bei umfangreicher und kompetenter Durchführung werden die Teilnehmer im Anschluss befähigt sein, sachkundig zu entscheiden, wie der Datenschutz geeignet umzusetzen ist, beziehungsweise ob sie in den jeweiligen Situationen einer Datenverarbeitung zustimmen sollten oder nicht.

Aus den vorgestellten Prinzipien des White Papers von CAUSE können viele Faktoren entnommen werden, die insbesondere bei einer zeitgemäßen Umsetzung des Datenschutzes an Universitäten von Bedeutung sind. Die neuen Problemfelder, die durch die vernetzen Informations- und Kommunikationssysteme entstehen, bedürfen nach CAUSE einer erneuten Auseinandersetzung mit dem Datenschutz. Das Umfeld, in dem die universitäre Lehre heute stattfindet, ist nicht mehr so präzise definierbar wie früher und macht eine Kontrolle von Datenschutzbestimmungen schwieriger. Der *Family Educational Rights and Privacy Act*, auf dem die Betrachtung basiert, wird unter dem Gesichtspunkt ubiquitärer, verteilter Technologien durch CAUSE neu bewertet.
Zusammenfassend lässt sich sagen, dass es eine Reihe wichtiger Kriterien gibt, die den Datenschutz entscheidend beeinflussen. Hierzu gehören der Kontext, in dem eine Datenverarbeitung durchgeführt wird, die Definition von personenbezogenen Daten und die Einstufung der Schutzwürdigkeit dieser Daten. Auch sollte eine Abschätzung dahingehend durchgeführt werden, wie aufwendig die Umsetzung der Datenschutzbestimmungen ist. Die genannten Faktoren müssen individuell berücksichtigt werden, um einen angemessenen Datenschutz bereitzustellen.

5.1.2.2 Sicherheits- und Datenschutzkriterien im eLearning

In der Arbeit von Yee et al. [Yee06] wird der Schutz von personenbezogenen Informationen des Lernenden bei der Verwendung von mobilen eLearning-Systemen untersucht. Mobile eLearning-Systeme sollen dabei einen Zugriff auf Lerninhalte unabhängig vom Standort und mittels einer Vielzahl von IT-Geräten ermöglichen. Als Grundlage für die Untersuchung verwenden die Autoren den „*Personal Information Protection and Electronic Documents Act of Canada*“. Darin sind die folgenden zehn Datenschutzgrundsätze enthalten, die als Anforderungen für den Datenschutz in Kanada gelten.

- *Accountability* (Zurechenbarkeit; Verantwortliche der Datenverarbeitung müssen Name und Anschrift angeben)
- *Indentifying Purposes* (Zweckbestimmung; Festlegung des Zwecks vor oder während der Datenerhebung; Betroffener kann Auskunft darüber verlangen)
- *Consent* (Einwilligung; betroffene Person ist in Kenntnis über die Datenverarbeitung zu setzen und ihre Zustimmung für die Verarbeitung ist einzuholen)
- *Limiting Collection* (Datensparsamkeit; nur erforderliche Informationen sollen erhoben werden)
- *Limiting Use, Disclosure, and Retention* (begrenzte Verwendung, Preisgabe und Aufbewahrungszeit; personenbezogene Daten sollen nur für den ursprünglichen Zweck verwendet werden, außer bei gesetzlichen Regelungen oder der Zustimmung der betroffenen Person)
- *Accuracy* (Korrektheit; personenbezogene Daten sollen so genau, vollständig und aktuell sein, wie für den Zweck notwendig)
- *Safeguards* (Schutzmaßnahmen; personenbezogene Daten sind der Sensibilität entsprechend zu schützen)
- *Openess* (Offenheit; leicht zugängliche Informationen über die Methoden und Richtlinien der Datenverarbeitung)
- *Individual Access* (Auskunft an die betroffene Person über die Datenverarbeitung und die Einsicht in die erhobenen Daten)
- *Challenging Compliance* (Überprüfung, ob die Datenschutzbestimmungen eingehalten werden)

Für diese Datenschutzanforderungen stellen Yee et al. Maßnahmen zusammen, die die Einhaltung der kanadischen Gesetzesbestimmungen unterstützen sollen. Nach Auffassung der Autoren sind die genannten Datenschutzanforderungen größtenteils durch datenschutzfreundliche Mechanismen abzudecken, die im Folgenden vorgestellt werden. Dabei geben Yee et al. nur beispielhafte Lösungen an und gehen nicht davon aus, dass die präsentierten Techniken eine optimale Lösung darstellen.

Secure Distributed Logs

Die erste Maßnahme zur Unterstützung des Datenschutzes von Yee et al., die nun vorgestellt wird, ist *Secure Distributed Logs*. Dabei werden Interaktionen zwischen den Benutzern und dem eLearning-System aufgezeichnet. Verschiedene Programme, die auf unterschiedlichen Computern ausgeführt werden, sollten dies vornehmen. Dadurch und durch eine sichere Verschlüsselung dieser Log-Dateien, die den Zeitpunkt, die Aktion und den Verursacher speichern, ist eine Modifikation oder Löschung nicht mehr unbemerkt möglich.

Platform for Privacy Preference (P3P)

Die Datenschutzerklärung, durch die eine Webseite ihren Umgang mit personenbezogenen Daten erläutert, kann durch P3P automatisch gelesen und ausgewertet werden. Dadurch wird der Benutzer in die Lage versetzt, seine eigenen Datenschutzanforderungen mit den Datenschutzrichtlinien der jeweiligen Webseite zu vergleichen. Entsprechen die Datenschutzrichtlinien nicht den Anforderungen des Benutzers, kann er gewarnt werden und dann selbst entscheiden, ob er diese Webseite trotzdem besuchen möchte, beziehungsweise auf deren Dienste zugreifen möchte oder nicht.

Die Definition der eigenen Datenschutz-Präferenzen erfolgt dabei mit Hilfe der Sprache APPEL. So kann der einzelne Benutzer beispielsweise die Art der Daten, den Zweck, die Dauer der Speicherung sowie die Weitergabe der Daten an Dritte festlegen.

Yee et al. sprechen P3P jedoch nur eine unzureichende Unterstützung des Datenschutzes zu. Da die Einhaltung der auf Webseiten und auch von eLearning-Systemen veröffentlichten Datenschutzerklärungen durch P3P nicht gesichert werden kann. Es kann nur gewährleistet werden, dass der Benutzer über den Inhalt der Datenschutzerklärung informiert wird, bevor er personenbezogene Daten über sich angibt. Technische Mechanismen, die dafür sorgen, dass die Organisation oder Webseite sich gemäß ihrer Datenschutzerklärung verhält, gehören nicht zum Umfang von P3P. So bietet P3P laut Yee et al. nur eine schwache Unterstützung des Datenschutzes und der Sicherheit, da es nur Datenschutzerklärungen überprüft und den Benutzer dann die weitere Entscheidung überlässt. Wenn die Anforderungen des Benutzers nicht mit den Forderungen des Dienstanbieters übereinstimmen, kann er nur durch das Verlassen der Webseite seine personenbezogenen Daten schützen.

Policy-based Approach for Privacy/Security Management

Dieses auf Regeln basierte Verfahren wird durch Berechtigungen und Verpflichtungen über Objekte und Subjekte realisiert. Es ermöglicht in verteilten eLearning-Systemen Aktionen und Zugriffe hinsichtlich Privatheit und Sicherheit anzupassen. So ist es in einem eLearning-System möglich, ein Set von Regeln für jede Benutzerrolle, wie Administrator, Lehrender, Lernender, aber auch für Kursmaterial festzulegen sowie für die Interaktionen zwischen diesen Subjekten und Objekten. Des Weiteren schlagen Yee et al. vor, dass Regierungseinrichtungen generelle Regelungen in dieses Rechtessystem einfließen lassen.

Network Privacy

Durch die offene Struktur des Internets und der Möglichkeit mit relativ geringem Aufwand Netzwerkkommunikationen abzuhören, können leicht auch als privat betrachtete Daten bei der Verwendung eines eLearning-Systems von Dritten abgehört werden. Eine gesicherte Übertragung kann nach Yee et al. mittels *Secure Sockets Layer* oder *Virtual Private Networks* realisiert werden.
Die Kommunikation an sich, die IP-Adresse und die Muster, die bei der Kommunikation entstehen, werden durch diese Technologien aber nicht geschützt. Um diese Kommunikationseigenschaften zu verschleiern, ist der Einsatz weiterer Technologien nötig. Eine Möglichkeit stellt hier die Verwendung eines Proxys dar. Mit Hilfe eines Proxys wird die Kommunikation zwischen dem Computer des Lernenden und dem Server der Anwendung über einen weiteren Computer im Netzwerk umgeleitet. Auf diese Weise erfolgt zwischen Benutzer und Server der Lernumgebung keine direkte Kommunikation mehr, sondern nur über den eingesetzten Proxy. Der Server ist dadurch nicht mehr in der Lage, die IP-Adresse des Benutzers der Lernplattform einzusehen. Der Proxy muss aber vertrauensvoll sein, oder sollte öfter gewechselt werden, da er die Kommunikation mitverfolgen kann. Auch wäre es einem Beobachter, der den Datenfluss des Netzwerks überwacht, leicht möglich, einzelne Datenspuren nach zu verfolgen. Durch zeitliche Verknüpfung eingehender und ausgehender Datenpakete beim Proxy könnte er ermitteln, welcher Benutzer welche Anfragen an den Server sendet. Einen wesentlich effektiveren Schutz stellen Technologien wie *MIX-Netzwerke*[1] oder *Crowds*[2] dar. Auch

[1] Siehe beispielsweise: http://www.bsi.bund.de/literat/anonym/mixmodel.htm
[2] Siehe beispielsweise: http://www.bsi.bund.de/literat/anonym/anwmix.htm#6.3

hier besteht die Grundidee darin, nicht direkt mit dem Dienstanbieter zu kommunizieren, sondern mehr oder weniger komplexe Zwischenstationen zu durchlaufen. Durch die Nutzung derartiger Zwischenstationen und dem zusätzlichen Einsatz kryptographischer Verfahren kann ein hohes Maß an Privatheit zur Verfügung gestellt werden. Im Gegensatz dazu steigt aber auch die Zeit, die für die Datenübertragung benötigt wird. Nutzt man kombiniert mehrere der oben genannten Technologien, kann die Sicherheit nochmals gesteigert werden. Jedoch ist diese wiederum mit gesteigertem Aufwand und damit langsameren Transferraten verbunden. Aus diesem Grund muss ein guter Kompromiss zwischen erreichter Anonymität und benötigter Performance für die Verwendung der eLearning-Anwendung gefunden werden. Nach Yee et al. ist es in den meisten Fällen schon ausreichend, wenn eine geschützte Übertragung, wie bei der Verwendung von SSL[1], genutzt wird.
Für eLearning-Systeme, die auch auf Mobiltelefonen und Personal Digital Assistence (kurz PDA) verwendet werden, ist der Schutz des Standortes des Benutzers besonders wichtig. Bei mobilem Zugriff auf ein Lernsystem kann nicht nur ein bestimmter Standort durch unbefugte ermittelt werden, sondern es können auch ganze Tagesabläufe und Bewegungsmuster bestimmt werden. Auch dies lässt sich durch die Techniken des Proxys, der *MIX-Netzwerke* und der *Crowds* schützen.

Trust Mechanisms

Eine weitere Technik, um die genannten Datenschutzanforderungen in verteilten eLearning-Systemen umzusetzen, sehen die Autoren in *Trust Mechanisms*. So ist gegenseitiges Vertrauen zwischen Dienstanbieter und Teilnehmer in dieser Umgebung notwendig. Einerseits müssen Lernende darauf vertrauen, dass der Dienstanbieter ihre personenbezogenen Informationen nur in der Art und Weise verarbeitet, wie in der Datenschutzerklärung angegeben wurde. Andererseits muss der Dienstanbieter seinerseits darauf vertrauen, dass diejenigen Teilnehmer, die das Lernangebot nutzen, auch diejenigen sind, die der Dienstanbieter dazu autorisiert hat. Die Autoren unterscheiden hier zwischen digitalen Zertifikaten und Trust Management Systemen, um Vertrauen zu etablieren. Digitale Zertifikate basieren dabei meist auf den Verfahren der *Public-Key Infrastructure* oder der *PGP* Spezifikation [Yee06]. Dadurch ist es möglich, Benutzer als vertrauensvoll zu definieren beziehungsweise deren Vertrauenswürdigkeit zu bestätigen. Techniken, die mit den aufgeführten Vertrauensmechanismen arbeiten, sind eMail-Verschlüsselung mittels PGP und Verbindungen, die SSL verwenden.
Trust Management Systeme bieten Vorteile bei der Definition und Kontrolle von Berechtigungen. So kann überprüft werden, ob eine angeforderte Aktion genehmigt wird oder nicht. Bekannte Trust Management Systeme sind unter anderem *KeyNote* und *REFEREE*. Durch diese Systeme lässt sich der Zugriff auf Ressourcen und Diensterbringungen regulieren.

eLearning-Spezifikationen

Von den Autoren werden weiterhin Spezifikationen vorgestellt, die für die Verwendung im eLearning-Kontext vorgesehen sind und sicherheits- und datenschutzunterstützende Maßnahmen bieten. Dabei wird speziell auf die Spezifikationen P1484.2 der IEEE und IMS LIP eingegangen.

IEEE P1484 ist eine Sammlung von Standards für Lerntechnologien, die vom IEEE LTSC entworfen wurden. IEEE P1484.2 stellt dabei eine Spezifikation für Lernerinformationen dar, die *Public And Private Information for Learners* kurz PAPI. In dieser Spezifikation wird ne-

[1] Secure Sockets Layer

ben dem Aufbau und Inhalt von Lerninformationen auch auf datenschutzfreundliche Funktionalitäten und Sicherheit eingegangen. Der genannte Standard ist zur Vereinheitlichung und zum Austausch von Lernerinformationen zwischen verschiedenen Systemen gedacht.
Für diesen Zweck werden Elemente definiert, die in einer Lernerinformation enthalten sein können und einen Lernenden und dessen Lernprozess charakterisieren. Dazu gehören Informationen über Fähigkeiten, Lernstil, Beziehungen zu anderen Benutzern, Präferenzen, Leistungen und Portfolios. Es ist möglich, die Granularität dieser Informationen einzustellen. Auf diese Weise erlaubt die Spezifikation beispielsweise für Lernende, Lehrer, Eltern oder Schulungseinrichtungen unterschiedliche Sichten auf die Lernereigenschaften. Außerdem kann so die Sicherheit und der Datenschutz von Lernerinformationen hinsichtlich verschiedener Interessengruppen angepasst werden. Dabei bietet die Spezifikation keine Unterstützung von konkreten Datenschutzanforderungen an, sondern stellt nur ein Gerüst für die Umsetzung von vielfältigen Datenschutz- und Sicherheitsanforderungen zur Verfügung [PAPI00].
Nach Meinung von Yee et al. werden durch diese Spezifikation viele der Datenschutzbedenken von Lernenden angesprochen. Besonders die Möglichkeit, Informationen zu anonymisieren oder zu partitionieren, vereinfacht den Datenschutz.

Die zweite vorgestellte Spezifikation für die Beschreibung von Lernerinformationen im e-Learning stellt das IMS Global Learning Consortium zur Verfügung. Auch hier wird eine Reihe von Spezifikationen entwickelt, die sich mit der Beschreibung von Metadaten, Inhaltsobjekten oder standardisierten Fragen und Tests auseinandersetzen. Dazu gehört das Learner Information Package (IMS LIP). Dies wurde primär entwickelt, um die Interoperabilität zwischen unterschiedlichen Systemen zu unterstützen. Es definiert wie PAPI auch das Ausmaß der Informationen, die über einen Lernenden gesammelt werden können und unterstützt die Organisation von Lernerinformationen.
Die IMS LIP Spezifikation ermöglicht eine Unterstützung des Datenschutzes und der Sicherheit. So ist ein *Learner Information Server* für den Austausch der Daten mit anderen Systemen verantwortlich und unterstützt den Eigentümer der Daten festzulegen, an wen welche Informationen weitergegeben werden dürfen.
Die Spezifikation enthält wiederum keine Implementierungsdetails für eine Datenschutzunterstützung, sondern stellt nur Strukturen zur Verfügung, die für jede passende Architektur zur Unterstützung von Datenschutz-Implementierung für Lernende genutzt werden können.
In der hierarchischen Beschreibung der Lernerinformation besitzt jeder Eintrag einen Anhang, in dem eine dazugehörige Beschreibung der Datenschutzanforderungen dieser Information enthalten ist. In dieser Beschreibung kann der Grad des Schutzes, die Zugriffsrechte und die Integrität der Daten definiert werden.
Außerdem wird eine *SecurityKey*-Datenstruktur zur Verfügung gestellt, in der Passwörter und kryptographische Schlüssel gespeichert werden, die für eine verschlüsselte Kommunikation, für den Beweis der Echtheit von Daten und für passwortbasierten Zugriff auf die Lernerinformationen verwendet werden können.

Auf weitere Standards im eLearning gehen Yee et al. nicht ein. Als Grund wird hierfür angegeben, dass weitere Spezifikationen, die die Verwaltung von Inhalten, Metadaten-Spezifizierung oder andere Bereiche des eLearning fokussieren, nur geringen Bezug zu Datenschutz und Sicherheit aufweisen.

Zusammenfassend lassen sich anhand der Techniken, die Yee et al. vorgestellt haben, Datenschutzanforderungen wie folgt erfüllen: Durch die Maßnahme der *Secure Distributed Logs* können die Datenschutzgrundsätze der *Accountability*, *Limiting Use/Disclose/Retention* und *Challenging Compliance* umgesetzt werden. Diese geschützt gespeicherten Log-Dateien ermöglichen die Überprüfung der Einhaltung der Datenschutzgrundsätze, beziehungsweise es

kann dadurch festgestellt werden, wann und durch wen diese verletzt wurden. Außerdem gehen die Autoren davon aus, dass sich jede weitere der genannten Datenschutzanforderungen indirekt dadurch unterstützen lässt.
P3P kann die Prinzipien des *Limiting Purposes*, *Consent* und *Openness* unterstützen. Wobei die Zustimmung eines Benutzers bei der Übereinstimmung der Datenschutzerklärung mit den Benutzeranforderungen implizit angenommen wird.
Bei dem *Policy-based Approach for Privacy/Security Management* können Regelungen über Berechtigungen die Datenschutzanforderungen *Limiting Collection* und *Individual Access* erfüllen. Verpflichtungen, die an bestimmte Aktionen und Objekte geknüpft sind, können außerdem zur teilweisen Realisierung der *Identifying Purpose*, *Consent*, *Limiting Use/Disclose/Retention*, *Safeguards* und *Openness* genutzt werden.
Durch *Network Privacy* können teilweise die Anforderungen *Limiting Collection*, *Individual Access* und *Safeguards* erfüllt werden.
Die Anforderungen der *Openness* und *Challenging Compliance* können auch mittels *Trust Mechanisms* erreicht werden. Des Weiteren ist eine teilweise Unterstützung der *Accountability*, *Accuracy*, *Safeguards* und *Individual Access* mittels dieser Methode möglich.

Nach Auffassung der Autoren lassen sich aber die Anforderungen der *Limiting Collection, Accuracy, Safeguards* und *Individual Access* nur indirekt durch die vorgestellten Maßnahmen erfüllen [Yee06]. Das Ziel der Autoren bei ihrer Untersuchung lag nicht in dem Aufzeigen optimaler Techniken für die Umsetzung der Datenschutzanforderungen. Sondern es sollten nur Beispiel-Techniken vorgestellt werden, die für die Erfüllung der Datenschutzkriterien als geeignet erschienen.

5.1.2.3 Sicherheit- und Datenschutzkriterien bei Lernmanagement-Systemen

In der Arbeit von Chan et al. [Cha03] werden Sicherheits- und Datenschutzanforderungen für webbasierte Lernsysteme aufgestellt und analysiert, wobei auch auf etwaige Risiken eingegangen wird. Des Weiteren werden zwei ausgewählte Lernmanagement-Systeme, Blackboard und WebCT, anhand erarbeiteter Bewertungskriterien evaluiert. Die Autoren stützen sich für ihre Betrachtung von webbasierten Lernplattformen auf Authentifikation, Zugriffskontrolle, Vertraulichkeit, Integrität und Nachweisbarkeit als Grundvorrausetzungen für die Sicherheit. Die Privatheit der Benutzer beruht laut den Autoren darauf, dass spezielle Benutzerinformationen, wie Profile von Lernenden und deren Verhalten sowie Prüfungsleistungen, nur durch autorisierte Personen und Gruppen eingesehen werden dürfen. Weiterhin kann laut Chan et al. eine Gleichbehandlung der Lernenden erzielt werden, wenn ihre Identitäten während der Prüfung und Notenvergabe gegenüber dem Bewertenden verborgen werden. Eine solche Herangehensweise würde die Privatheit der Betroffenen gewährleisten.

Gegenüber der klassischen Lehre kommen durch die Verlagerung von Lehrveranstaltung in eine vernetze Umgebung zusätzliche Gefahren für die Sicherheit hinzu: Die Autoren führen an, dass es durch schwache Passwörter oder die Weitergabe von Login-Daten anderen Personen als dem eigentliche Inhaber eines Logins gestattet wird, Zugang zu Lehrveranstaltungen und Prüfungen zu erhalten. Darüber hinaus ist die Anonymität während der Bewertung von Lernenden gegenüber dem Bewertenden nicht automatisch gegeben und es existieren generell Gefahren, die die Sicherheit in webbasierten Systemen beeinträchtigen können.
Als Schutz gegen die beschriebenen Gefahren schlagen Chan et al. unter anderem Maßnahmen wie die Verwendung von SSL-Verschlüsselung vor, um die Vertraulichkeit bei der Datenübertragung zu gewähren. Aber auch die Implementierung von sicheren Mechanismen zur Authentifizierung verringert die beschriebenen Gefahren.

5.2 Kriterien für diese Evaluation

In dem vorhergehenden Abschnitt dieses Kapitels sind Kriterien für eine Bewertung des Datenschutzes an Software-Systemen und von Umgebungen, die das vernetze Lernen und Lehren unterstützen, vorgestellt worden. Es konnten Anforderungen identifiziert werden, die besonders beim eLearning zu beachten sind. Nun sollen aus diesen Erkenntnissen Bewertungskriterien für die eigene Untersuchung abgeleitet werden.

5.2.1 Kriterium: Datensparsamkeit

Ein wesentlicher Grundgedanke, der sowohl von den meisten betrachteten Quellen als auch von den vorgestellten Gesetzen als Grundlage für den Datenschutz, aufgeführt wurde, ist der Aspekt der Datensparsamkeit. Die Menge der Daten, die gesammelt werden, ist auch bei einem Lernmanagement-System von Bedeutung. Hier sollen folgende Kriterien betrachtet werden:

- Anonyme und pseudomyme Verwendung der Lernplattform,
- Konfigurationsmöglichkeiten.

Bei der Betrachtung eines Lernmanagement-Systems unter dem Aspekt der Datensparsamkeit soll auf die Fragestellung genauer eingegangen werden, welche personenbezogenen Daten für die Durchführung der Lehre mit Hilfe einer Lernplattform wirklich notwendig sind. In einer Lernplattform können persönliche Angaben bei der Anmeldung verlangt werden oder durch Zugriff auf bestehende Datenbanken, die personenbezogene Daten enthalten, auch in der Lernplattform ohne das Mitwirken den Benutzers zur Verfügung gestellt werden. In der Definition zu Lernmanagement-Systemen, die in Kapitel 2 erarbeitet wurde, ist auch das Mitverfolgen von Lernaktivitäten eine Grundfunktionalität, die von Lernplattformen angeboten wird. Je nach Granularität dieser Aufzeichnungen kann dadurch das Verhalten einzelner Benutzer sehr genau festgehalten werden. So kann eine Anonymisierung oder Pseudonymisierung des Zugriffs, wie es beispielsweise in [ULD05] vorgeschlagen wird, sich auch für Lernumgebungen als sinnvoll erweisen, um die Privatsphäre der Benutzer insbesondere der Lernenden zu schützen. Des Weiteren soll analysiert werden, ob und welche Konfigurationen bei der Datenerhebung vorgesehen sind. Dieser Aspekt stellt ebenfalls ein Untersuchungskriterium von [ULD05] dar.

5.2.2 Kriterium: Zweckbestimmung und Nutzungsbegrenzung

Nachdem personenbezogene Daten erhoben wurden, ist es nach den vorgestellten Datenschutzrichtlinien und Veröffentlichungen notwendig, dass der Zweck der Datenverarbeitung eingehalten wird und die Informationen nicht darüber hinaus verarbeitet werden. Um die konkrete Umsetzung in den ausgewählten Lernmanagement-Systemen zu betrachten, sollen folgende Kriterien untersucht werden:

- Zweckbestimmung vor der Erhebung,
- Einschränken der Verarbeitung,

- Löschen oder Anonymisieren von personenbezogenen und sensiblen Informationen nach Wegfall der Erforderlichkeit.

Dabei soll geprüft werden, ob Funktionen zur Verfügung gestellt werden, die die Festlegung des Zwecks vor der Datenverarbeitung gestatten, wie es beispielsweise in [CAU97] verlangt wird, sowie die Einhaltung des Zwecks überwachen. Dies wird unter anderem auch im Anforderungskatalog des ULD aufgeführt.
Ein Lernmanagement-System könnte beispielsweise eine Funktion anbieten, mit deren Hilfe die Zwecke der Datenverarbeitung vor der Erhebung konfiguriert und durch das Programm protokolliert werden können. So könnte überwacht werden, ob Daten über den eigentlichen Zweck hinaus unrechtmäßig weiterverarbeitet werden, wenn sie zum Beispiel mit anderen Datenbanken verknüpft werden oder eine Weitergabe an unberechtigte Dritte erfolgt.
Die Nutzungsbegrenzung wird dann unterstützt, wenn auf Daten, für die keine Erforderlichkeit mehr besteht, nicht mehr oder nur noch eingeschränkt zugegriffen werden kann. Das Löschen von personenbezogenen Daten, die nicht mehr erforderlich sind, wird vom ULD [ULD05] und von CAUSE [CAU97] als mögliche Maßnahme dafür vorgeschlagen.

5.2.3 Kriterium: Rollen und Zugriffsrechte

Ein Rollenkonzept, in dem Benutzern des Lernmanagement-Systems unterschiedliche Rechte eingeräumt werden, ist eine der Grundvoraussetzungen, die eine Lernplattform kennzeichnen (siehe die gewählte Definition in Kapitel 2). Diese Rollen und Rechte können auf die Informationelle Selbstbestimmung anderer Benutzer großen Einfluss nehmen. Dabei sind folgende Kriterien eingehender zu betrachten:

- Rollen- und Rechtevergabe,
- Umsetzung der Rollen und Rechte,
- Transparenz bei den Auswirkungen auf die Privatheit anderer Benutzer.

Da die Vergabe von einzelnen Rechten sowie kompletter Rollen viel Verantwortung erfordert, soll betrachtet werden, wie diese vergeben werden. Hier soll auch untersucht werden, ob die Lernplattform den Benutzern transparent macht, welche Rollen welche konkreten Rechte beinhalten. Besonders ist dies zu beachten, wenn Rechte zu individuellen Rollen zusammengefügt werden können. Ein weiterer Aspekt soll die Analyse sein, welche datenschutzrelevanten Rechte den jeweiligen Rollen überhaupt in den einzelnen Lernmanagement-Systemen zugeordnet werden und insbesondere welche Rolle welche personenbezogenen Daten einsehen darf. Der genannte Fragekomplex wird beispielsweise in dem *Need to Know* Prinzip in [CAU97] andiskutiert.

5.2.4 Kriterium: Rechte des Betroffenen und Informationelle Selbstbestimmung

Hier soll die Rechtmäßigkeit der Datenverarbeitung untersucht werden. Nach den vorgestellten Gesetzen ist für eine rechtmäßige Datenverarbeitung entweder die Einwilligung des Betroffenen notwendig, oder der Datenverarbeiter wird anderweitig rechtlich dazu befugt (siehe Kapitel 3). Insbesondere das ULD erachtet dieses Kriterium als sehr wichtig, indem es dieses Thema in zwei der vier vorgestellten Komplexe behandelt.

Darüber hinaus soll hier betrachtet werden, wie viel Entscheidungsgewalt jeder Benutzer bei der Mitgestaltung der Datenverarbeitung hat und ob das Recht auf Informationelle Selbstbe-

stimmung unterstützt wird. Zu klären ist beispielsweise, wie der Betroffene durch die Lernplattform über seine personenbezogenen Daten informiert wird. Folgende Kriterien stehen hier im Vordergrund:

- Unterstützung des Einwilligungsprozesses,
- Unterstützen der Anfertigung und Platzierung einer Datenschutzerklärung,
- Informieren über die Durchführung der Datenverarbeitung,
- Einsicht von persönlichen Informationen durch den Betroffenen,
- Einsicht von Benutzeraktivitäten durch den Betroffenen,
- Überprüfen der Einhaltung der Datenschutzerklärung,
- Modifikation personenbezogener Daten durch den Betroffenen,
- Mitbestimmung der Datenverarbeitung durch den Betroffenen,
- Unterstützung von datenschutzförderlichen Spezifikationen,
- Sensibilisierung der Benutzer.

Dabei soll bewertet werden, wie gut der Einwilligungsprozess durch die einzelnen Lernmanagement-Systeme unterstützt wird und ob und in welcher Form eine Datenschutzerklärung integriert werden kann. Dies stellt auch einen Untersuchungspunkt beim Gütesiegel-Verfahrens des ULD dar. Dazu gehören auch die Unterstützung des Widerrufs, der Änderung bei inkorrekten Angaben und die Benachrichtigung des Betroffenen, wenn sich die Konditionen der Datenverarbeitung ändern. In einer Datenschutzerklärung kann der Betroffene Angaben zu Informationen über den Anbieter, die Datenarten, den Zweck und die Sicherheitsvorkehrungen der Datenverarbeitung einsehen.
Da Lernmanagement-Systeme in der Lehre verwendet werden, ist ein Einsatz auch in Schulen denkbar. Nach der Betrachtung der Datenschutzgesetze Minderjähriger (siehe Kapitel 3) ist aber eine umfassende Einwilligung durch Schüler nicht immer rechtskräftig. Es ist zu untersuchen, ob und wie Lernmanagement-Systeme auf diese Problematik eingehen.
Als ein weiterer zu untersuchender Aspekt soll die Bereitstellung von Auskünften bezüglich personenbezogener Daten der Betroffenen betrachtet werden. Dabei soll auf zwei Formen von personenbezogenen Daten eingegangen werden. Die erste Form sind die Primärdaten, die persönliche Informationen enthalten und die eine Person direkt identifizieren können. Die zweite Form beinhaltet Informationen über Konfigurationen, die ein Benutzer vornimmt, Zugriffe auf Objekte in dem Lernmanagement-System und Aktivitätsdaten, die protokolliert werden. Zu klären ist außerdem, ob Techniken und Maßnahmen zur Verfügung gestellt werden, die es erlauben, die Einhaltung der Datenschutzerklärung und damit ihre Rechtmäßigkeit zu überprüfen. Dies ist auch ein Datenschutzkriterium, das in [ULD05] analysiert wird.
In den in [Yee06] vorgestellten Spezifikationen für eLearning-Systeme, wird auf Datenschutzaspekte für Lernerprofile eingegangen. Dazu gehören nach Yee et al. das *IMS Learner Information Package* und *IEEE Public and Private Information*. Es soll untersucht werden, ob diese Spezifikationen in den zu untersuchenden Lernmanagement-Systemen unterstützt werden.
Außerdem soll das Mitspracherecht der Benutzer hinsichtlich der Datenverarbeitung analysiert werden. So sollte ein Benutzer selbst festlegen können, welche Daten über ihn gesammelt werden dürfen, zu welchem Zweck und wer diese einsehen darf. Darüber hinaus wäre es für die Informationelle Selbstbestimmung interessant für einen Benutzer einzusehen, ob und wer auf personenbezogene Informationen über ihn zugegriffen hat. Beispielsweise werden in [CAU97] insbesondere beim Prinzip *Nondisclosure and Consent* der Einbezug des Studenten in einzelne Bereiche der Datenverarbeitung diskutiert.
Zuletzt kann auch eine Lernplattform ihre Benutzer für den Datenschutz sensibilisieren. Dies könnte durch geeignet platzierte Hinweise, vorgefertigte Datenschutzkurse oder durch Erläuterungen in der Online-Hilfe beziehungsweise im Handbuch geschehen. Dieses Kriterium der

Sensibilisierung wird auch in [ULD05] und [CAU97] bei dem Prinzip *Education* als wichtiger Bestandteil des Datenschutzes dargestellt.

5.2.5 Kriterium: Sicherheit und Datenqualität

In den bisherigen Betrachtungen zum Datenschutz wurde herausgearbeitet, dass Sicherheit als eine Grundvoraussetzung für den Datenschutz und die Informationelle Privatheit angesehen wird. Deshalb soll auch die Datenschutzbewertung von Lernmanagement-Systemen diesbezügliche Sicherheitsmaßnahmen untersucht werden. Folgende Kriterien sollen dabei berücksichtigt werden:

- Datenübertragung,
- Speicherung,
- Authentifizierung,
- Protokollierung für die Überwachung des Sicherheitszustandes,
- Schutz vor unbefugter Löschung, Einsicht und Modifikation,
- Qualität der Daten hinsichtlich Richtigkeit, Vollständigkeit und Aktualität.

Da ein Lernmanagement-System meist verteilt über das Internet angeboten wird, sind Sicherheitsmaßnahmen zu ergreifen, die es unbefugten Personen nicht ermöglichen, Zugriff auf personenbezogene Informationen zu erhalten. Es soll untersucht werden, ob und wie Datenübermittlung, Datenhaltung und Zutritt zum Lernmanagement-System hinsichtlich Datenschutzes gestaltet sind und wer berechtigt ist, Einstellungen vorzunehmen. Das Lernmanagement-System kann auch eine Kategorisierung von personenbezogenen Daten unterstützen, wobei je nach Kategorie unterschiedliche Schutzmechanismen zur Anwendung kommen. Weiterhin kann durch die Protokollierung von Benutzerzugriffen der Sicherheitszustand der Lernplattform überwacht werden und nachträglich sicherheitsrelevante Ereignisse dem Verursacher zugeordnet werden. Personenbezogene Daten sollten außerdem vor unbefugter Modifikation und Einsicht geschützt sein. Darüber hinaus sollten sie, wenn benötigt, korrekt, aktuell und vollständig sein. In den vorgestellten Veröffentlichungen wird dem Thema Sicherheit große Bedeutung beigemessen. So wird in [ULD05] geprüft, welche Sicherheitsmaßnahmen zum Einsatz kommen und ob diese dem Kontext angemessen sind. Auch bei CAUSE [CAU97], Yee et al. [Yee06] und Chan et al. [Cha03] wird sich mit der Sicherheit in Bildungssystemen, eLearning-Systemen und Lernplattformen auseinandergesetzt.

5.3 Zusammenfassung

In diesem Kapitel wurden Quellen aus angrenzenden Gebieten vorgestellt. In diesen werden viele Kriterien vorgestellt, die sich meist an den jeweils relevanten Gesetzen orientieren. Obwohl sie auf unterschiedlichen Grundlagen basieren, gibt es einige Grundanforderungen für den Datenschutz.
Hinsichtlich Bewertungskriterien für die eigene Untersuchung wurden diese Grundanforderungen identifiziert und mit Kriterien, die als besonders relevant für die Datenschutzbewertung von Lernmanagement-Systemen eingestuft werden, verknüpft.
Die Bewertungskriterien und die dafür zu untersuchenden Teilgebiete werden hier nochmals tabellarisch (Tabelle 5.1) zusammengefasst:

Datensparsamkeit	• Anonyme und pseudomyme Verwendung der Lernplattform, • Konfigurationsmöglichkeiten.
Zweckbestimmung und Nutzungsbegrenzung	• Zweckbestimmung vor der Erhebung, • Einschränken der Verarbeitung, • Löschen oder anonymisieren von personenbezogenen und sensiblen Informationen nach Wegfall der Erforderlichkeit.
Rollen und Zugriffsrechte	• Rollen- und Rechtevergabe, • Umsetzung der Rollen und Rechte, • Transparenz bei den Auswirkungen auf die Privatheit anderer Benutzer.
Rechte des Betroffenen und Informationelle Selbstbestimmung	• Unterstützung des Einwilligungsprozesses, • Unterstützen der Anfertigung und Platzierung einer Datenschutzerklärung, • Informieren über die Durchführung der Datenschutzverarbeitung, • Einsicht von persönlichen Informationen durch den Betroffenen, • Einsicht von Benutzeraktivitäten durch den Betroffenen, • Überprüfen der Einhaltung der Datenschutzerklärung, • Modifikation personenbezogener Daten durch den Betroffenen, • Mitbestimmung der Datenverarbeitung durch den Betroffenen, • Unterstützung von datenschutzförderlichen Spezifikationen. • Sensibilisierung der Benutzer.
Sicherheit und Datenqualität	• Datenübertragung, • Speicherung, • Authentifizierung, • Protokolle für die Überwachung des Sicherheitszustandes, • Schutz vor unbefugter Löschung Einsicht und Modifikation, • Qualität der Daten hinsichtlich Richtigkeit, Vollständigkeit und Aktualität.

Tabelle 5.1: Übersicht über die Bewertungskriterien

6. Ergebnisse der Untersuchung

In diesem Kapitel werden die Ergebnisse der Datenschutzuntersuchung vorgestellt. Im ersten Abschnitt wird das Vorgehen beschrieben, wie die Ergebnisse für die einzelnen Bewertungskriterien ermittelt wurden. Dabei wird insbesondere auf die Befragung der Zielgruppe zu den Bewertungskriterien eingegangen. Der zweite Abschnitt befasst sich mit der konkreten Vorstellung einzelner Ergebnisse aus den jeweiligen Untersuchungsarten bezüglich der Lernmanagement-Systeme. Außerdem wird hier eine Kategorisierung der Lernmanagement-Systeme im Hinblick auf Datenschutzaspekte vorgestellt. Eine Gegenüberstellung der Ergebnisse der einzelnen Lernmanagement-Systeme auf Grundlage der Bewertungskriterien findet im dritten Abschnitt statt. Dabei soll auch ein Konzept für eine Lernplattform zusammengestellt werden, die die Datenschutzkonzepte der einzelnen Lernmanagement-Systeme bündelt. Im vierten Abschnitt werden die Untersuchungsergebnisse der Studie [Sta06] hinsichtlich der Wünsche der Benutzer von eLearning-Systemen mit den Ergebnissen in dieser Arbeit vergleichen, die die Unterstützung der Informationellen Selbstbestimmung in den untersuchten Lernmanagement-Systemen wiedergeben. Abschließend werden in Abschnitt 5 die Ergebnisse noch einmal zusammengefasst.

6.1 Allgemeine Beobachtungen

Als erster Schritt für die Durchführung der Datenschutzbewertung wurde ein Fragebogen angefertigt, der die in Kapitel 5 gewonnenen Bewertungskriterien in Form von ausformulierten Fragestellungen enthält. Dieser setzt sich aus mehreren Fragekomplexen zusammen und enthält neben ja/nein-Fragen, die die Erfüllung bestimmter Kriterien abfragen, auch Fragen mit Freitext-Antworten, bei denen die Umsetzung der erfüllten Kriterien zu beschreiben ist. Der vollständige Fragebogen ist in Anhang B zu finden.

Der Fragebogen wurde in Form eines digitalen Formulars an Anbieter, Entwickler und Administratoren der ausgewählten Lernmanagement-Systeme gesendet mit der Bitte, diesen ausgefüllt zurückzusenden. Gegebenenfalls wurde der Fragebogen auch im direkten Gespräch beantwortet, wenn sich dies anbot. Die Ansprechpartner sind durch eine Internet-Recherche der ausgewählten Lernplattformen an Universitäten ermittelt worden. Des Weiteren wurden Anbieter auch direkt per eMail kontaktiert. Für die Befragung sind 31 Personen und Institutionen per eMail angeschrieben worden, die entweder ein Lernmanagement-System anboten oder den Support in Universitäten und Fachhochschulen für das bereitgestellte Lernmanagement-System sicherstellen. Insgesamt antworteten von diesen 31 Angeschriebenen fast 20 Personen, aber nur sieben sendeten auch den ausgefüllten Fragebogen zurück oder waren bereit für ein Interview.
Einerseits sind die Ursachen für den geringen Rücklauf in der sehr speziellen Zielgruppe zu suchen, die allgemein sehr schwierig zu ermitteln ist und nur einen kleinen Personenkreis darstellt. So haben in der der Studie „Privacy in eLearning“, die europaweit durchgeführt wurde, nur fünf von 107 Befragten angegeben, die Rolle eines Administrators in einem e-Learning-System zu bekleiden [Sta06]. Für die hier durchgeführte Befragung von deutschen Administratoren von Lernmanagement-Systemen ist somit das Resultat der Antworten - verglichen mit der Studie [Sta06] - relativ positiv zu bewerten. Andererseits können die Gründe für den geringen Rücklauf der beantworteten Fragebögen aus den eMail-Antworten entnommen werden. So ist es beispielsweise vorgekommen, dass durch das Anschreiben nicht der geeignete Ansprechpartner erreicht wurde oder es eine kompetentere Person in der Umgebung

des Angeschriebenen gab und die Anfrage weitergeleitet wurde. Leider wurden einige der weitergeleiteten eMails nicht beantwortet. Außerdem wurde geschildert, dass deutschlandweit das zu bewertende Lernmanagement-System nur durch eine Installation vertreten ist, die von einem Zusammenschluss von Universitäten benutzt wird und somit auch nur ein Ansprechpartner für dieses zur Verfügung steht. Es kam auch vor, dass das Lernmanagement-System an der angeschriebenen Institution nur sehr geringfügig eingesetzt wird oder geplant wird, dieses durch ein anderes zu ersetzen und dadurch von einer Beantwortung des Fragebogens abgesehen wurde. Nicht zuletzt wurden teilweise als Antwortschreiben sehr kurze Angaben zum eingesetzten Lernmanagement-System gemacht, die für die Untersuchung nicht verwendet werden konnten.

Die Resonanz allgemein auf die Datenschutzbewertung von Lernmanagement-Systemen fiel gemischt aus. So gab es einerseits Antworten, die großes Interesse an der Thematik bekundeten. So wurde es beispielsweise begrüßt, dass „das Thema Datenschutz im eLearning nach jahrelanger Vernachlässigung zunehmend an Bedeutung gewinnt“. Es wurde auch auf eigenständig durchgeführte Projekte im eLearning hingewiesen, um den Datenschutz in dem jeweiligen Lernmanagement-System zu verbessern. In einer anderen Antwort wird mitgeteilt, dass bezüglich des Datenschutzes von Lernmanagement-Systemen bisher keine Analysen stattgefunden haben und deshalb auch keine objektive Bewertung von Lernmanagement-Systemen aufgrund des Datenschutzes möglich ist. Auch aus einer weiteren Zusendung ist zu entnehmen, dass der Datenschutz zu den „völlig unterbelichteten Themen im Umfeld E-Learning“ gehört. Dabei gab es auch hier schon eine Auseinandersetzung mit dem Datenschutz. So wurde geäußert, dass die „Datenschutzgesetzgebung in Deutschland auf Länderebene liegt und unterschiedliche Regelungen für Schulen, Hochschule, Verwaltungen, freie Bildungsanbieter und Unternehmen (Betriebsvereinbarungen) gelten“. Auch können sich auf europäischer Ebene durch die unterschiedliche Ausgestaltung nationaler Gesetze Probleme in multinationalen eLearning-Projekten ergeben, die Lernmanagement-Systeme verwenden.

Andererseits kam es auch vor, dass ein Administrator eines Lernmanagement-Systems dem Datenschutz bisher keine Relevanz zugeschrieben hatte und sich praktisch bisher noch nicht mit diesem Themenfeld beschäftigt hat. Andere gaben an, dass das Lernmanagement-System nicht für Prüfungszwecke vorgesehen ist oder es keine schutzwürdigen, personenbezogenen Daten in dem Lernmanagement-System geben würde und somit auch keine besonderen Datenschutzmaßnahmen ergriffen werden müssten.
Weiterhin wurde angegeben, dass es nur unzureichende Unterrichtungen zum Thema Datenschutz gäbe und die verantwortlichen Administratoren nicht genügend zur Einhaltung des Datenschutzes geschult wären. Anhand dieser Aussagen kann eine gewisse Unsicherheit der Verantwortlichen beim Thema Datenschutz identifiziert werden, die entweder aus mangelnder Aufklärung oder durch die unklare Gesetzeslage und individuelle Interpretation der Datenschutzgesetze resultiert. Dies bedeutet, dass die Sensibilisierung der Mitarbeiter fehlt oder ihnen keine geeigneten Mittel in die Hand gegeben werden, den Datenschutz sicherzustellen.
Die geringe Rücklaufquote der Befragung kann auch durch den Aspekt der Unsicherheit mit beeinflusst sein, da für die Angeschriebenen dadurch wenig Motivation bestand, den Fragebogen auszufüllen und eventuell eigene Fehler aufzudecken.

6.2 Auswertung anhand der einzelnen Lernmanagement-Systeme

In diesem Abschnitt werden die Ergebnisse der durchgeführten Untersuchung bezüglich dem Datenschutz vorgestellt. Die Untersuchung jedes Lernmanagement-Systems wurde in vier Teile gegliedert: Zunächst werden im Abschnitt „Fragebogenantworten“ die Resultate aus der durchgeführten Befragung vorgestellt. Darin werden allgemeine Informationen, ob und wie die aufgestellten Bewertungskriterien erfüllt werden, aus Sicht der jeweiligen Befragten dargestellt. Es wird dabei nur auf die wichtigsten Angaben eingegangen. Die kompletten Antworten der befragten Administratoren, Entwickler und Anbieter befinden sich in tabellarischer Form in Anhang C. Im Anschluss daran werden im Abschnitt „Praxistest“ die eigenen Erfahrungen mit der Software geschildert. Dabei wird insbesondere auf die Umsetzung von Funktionalitäten, die den Datenschutz beeinflussen, eingegangen. Im dritten Abschnitt „Recherche weiterer Quellen“ werden Veröffentlichungen und Artikel vorgestellt, die sich ebenfalls mit dem entsprechenden Lernmanagement-System auseinandergesetzt haben. Diese Betrachtung dient zur Abrundung der Datenschutzanalyse und soll die dargestellten Ergebnisse komplettieren. Abschließend wird jedes Lernmanagement-System nochmals kurz eingeschätzt und auf datenschutzrelevante Besonderheiten eingegangen.
Im Anschluss daran soll eine Kategorisierung der Lernmanagement-Systeme vorgenommen und die jeweiligen Auswirkungen auf den Datenschutz aufgezeigt werden.

6.2.1 Blackboard

Fragebogenantworten

Die nachfolgenden Ergebnisse beziehen sich auf Blackboard Version 7.2. Die zugrunde liegende Installation wird durch die Universität Potsdam zur Verfügung gestellt und hat etwa 9000 angemeldete Benutzer. Die folgenden Informationen beinhalten die Antworten eines dort zuständigen Blackboard-Administrators zu den vorgestellten Bewertungskriterien.

Datensparsamkeit: Eine pseudonyme beziehungsweise anonyme Benutzung der Lernplattform ist nicht vorgesehen. Nach Meinung des Befragten werden durch Blackboard mehr sensible personenbezogene Informationen gesammelt als notwendig. Auch eine Weiterverarbeitung von Verkehrsdaten wird durch das Lernmanagement-System vorgenommen.

Zweckbestimmung und Nutzungsbegrenzung: Eine Zweckbestimmung vor der Datenerhebung des Lernmanagement-Systems wird durchgeführt.
Die Nutzungsbegrenzung wird dadurch unterstützt, dass es nur Personen möglich ist auf persönliche Informationen anderer Benutzer zuzugreifen, die diese für die Erfüllung ihrer Aufgaben benötigen. Des Weiteren werden personenbezogene Informationen nicht mit Daten aus anderen Datenbanken verknüpft. Die Möglichkeit zur Löschung von personenbezogenen Daten wurde ebenfalls angegeben, aber ohne eine Konkretisierung der diesbezüglichen Maßnahmen zu nennen.

Rollen und Zugriffsrechte: Laut dem Befragten bietet Blackboard mehrere Rollen an und stellt deren Rechte und Verpflichtungen sicher. Diese Rollen werden nur durch Personen vergeben, die entsprechend autorisiert sind. Welche Auswirkungen die Rollen und die damit verbundenen Rechte im Hinblick auf die Privatheit der betroffen Benutzer haben, ist für die Beteiligten nicht ersichtlich.

Rechte des Betroffenen und Informationelle Selbstbestimmung: Der Einwilligungsprozess kann durch das Lernmanagement-System unterstützt werden. Dabei wird der Benutzer bei Veränderungen der Konditionen informiert, kann aber die Einwilligung nicht widerrufen. Das Anfertigen und Plazieren einer Datenschutzerklärung wird ebenfalls unterstützt. Der Benutzer wird über die Datenkategorien, den Verantwortlichen, den Zweck, die Sicherheitsvorkehrungen der Datenverarbeitung und über die Weitergabe von personenbezogenen Daten informiert. Eine Überprüfung, ob die in der Datenschutzerklärung gemachten Zusicherungen eingehalten werden, kann durch die Benutzer nicht durchgeführt werden. Der Benutzer kann seine eigenen persönlichen Daten direkt in der Lernplattform einzusehen und diese zu modifizieren.
In Blackboard kann ein Benutzer selbst darüber entscheiden, welche seiner persönlichen Informationen er anderen Benutzern der über sich zur Verfügung stellt. Allerdings kann der Benutzer nicht selbst entscheiden, welche Daten und zu welchem Zweck über ihn gespeichert werden sollen. Ob und wann andere Benutzer die eigenen persönlichen Daten abgerufen, ist für den Benutzer nicht ersichtlich. Laut den Angaben des Befragten werden die in Kapitel 5 vorgestellten Spezifikationen IEEE PAPI und IMS LIP durch Blackboard unterstützt. Ob eine Sensibilisierung in Bezug auf den Schutz personenbezogener Daten durch die Lernplattform erreicht wird, konnte durch den Befragten nicht eingeschätzt werden.

Sicherheit und Datenqualität: Eine geschützte Datenübertragung ist bei Blackboard durch die Verwendung von SSL möglich. Auch eine gesicherte Speicherung von personenbezogenen Daten ist gewährleistet. Die Möglichkeit, bei diesen Schutzmaßnahmen Konfigurationen vorzunehmen, wird nur autorisierten Personen zur Verfügung gestellt, die dies global für alle Teilnehmer einstellen.
Der Zugriff auf die Lernplattform kann so gestaltet werden, dass er nur nach Authentifizierung der Benutzer möglich ist.
Eine Protokollierung von Benutzeraktivitäten zur Überwachung des Sicherheitszustandes wird nicht durch die Lernplattform angeboten. Aber das Lernmanagement-System bietet einen Schutz vor unautorisierter Löschung, Einsicht und Modifikation von personenbezogenen Daten. Dass die Informationen, die über einen Benutzer gesammelt werden, sachlich richtig sind, kann laut dem Befragten durch die Lernplattform gewährleistet werden.

Praxistest

Rechte des Betroffenen und Informationelle Selbstbestimmung: Blackboard konnte nur geringfügig anhand von Gastzugängen und Demokursen getestet werden. Dabei konnte lediglich eine datenschutzrelevante Funktionalität von Blackboard getestet werden. So ist es möglich, dass der Lernende seine persönlichen Angaben selbst bearbeiten kann. Außerdem kann er innerhalb von Blackboard einstellen, ob seine persönlichen Angaben allen Blackboard-Benutzern dieser Installation zugänglich gemacht werden sollen (siehe Abbildung 6.1). Dies unterstützt den Benutzer bei der Ausübung seines Rechtes auf Informationelle Selbstbestimmung und gibt ihm somit die Möglichkeit, die Datenverarbeitung seiner personenbezogenen Daten - wenn auch geringfügig - mit zu beeinflussen.

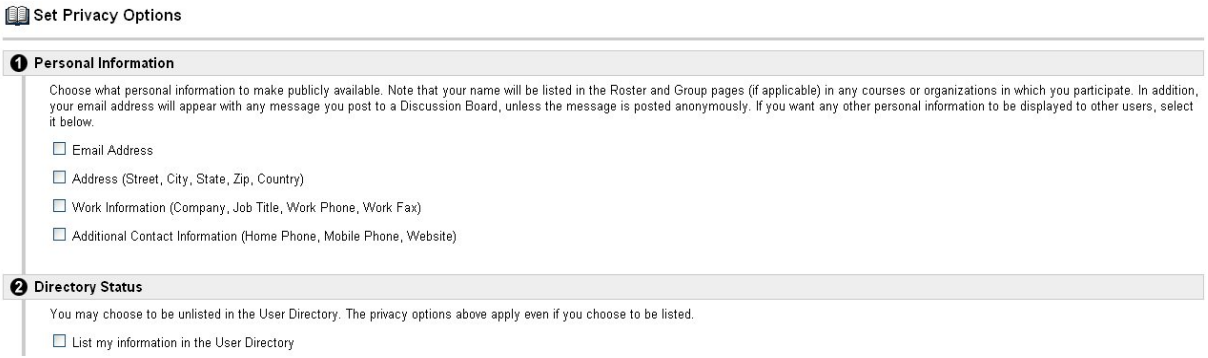
Set Privacy Options
1 Personal Information
Choose what personal information to make publicly available. Note that your name will be listed in the Roster and Group pages (if applicable) in any courses or organizations in which you participate. In addition, your email address will appear with any message you post to a Discussion Board, unless the message is posted anonymously. If you want any other personal information to be displayed to other users, select it below.
Email Address
Address (Street, City, State, Zip, Country)
Work Information (Company, Job Title, Work Phone, Work Fax)
Additional Contact Information (Home Phone, Mobile Phone, Website)
2 Directory Status
You may choose to be unlisted in the User Directory. The privacy options above apply even if you choose to be listed.
List my information in the User Directory

Abbildung 6.1: Konfiguration um persönliche Informationen öffentlich in Blackboard zugänglich zu machen

Recherche weiterer Quellen

Neben WebCT wird in [Cha03] auch Blackboard evaluiert. Die Kriterien dieser Evaluation wurden bereits in Kapitel 5 vorgestellt. Sicherheits- und Datenschutzeigenschaften von Blackboard werden dabei wie folgt bewertet:

- Authentifikation: Es wird nur eine passwortbasierte Authentifizierung angeboten. Dabei werden Cookies verwendet, die es ermöglichen, dass der Benutzer bei der Verwendung desselben Browsers sich nicht erneut anmelden muss. Wenn der Computer auch von anderen Personen verwendet wird, stellt dies eine Gefahr dar und kann einen unberechtigten Zugang ermöglichen.
- Zugriffskontrolle: Blackboard verwendet eine rollenbasierte Autorisierung.
- Vertraulichkeit: Das Lernmanagement-System unterstützt verschlüsselte Übertragung mittels Secure Shell Protokoll (SSL).
- Integrität: Es werden keine digitalen Signaturen unterstützt.
- Nachweisbarkeit: Um dies zu realisieren werden durch Blackboard Aktivitätsdaten gespeichert.
- Privatheit: Der Benutzer kann seine eigenen Einstellungen bezüglich Privatheit vornehmen und hat somit die Kontrolle über die Preisgabe seiner persönlichen Informationen. Aber Anonymität des Lernenden gegenüber dem Bewertenden während der Durchführung von Prüfungen ist nicht vorgesehen.

In Blackboard ist es möglich, mehrmals mit demselben Benutzerkonto angemeldet zu sein. Dies stellt nach Chan et al. eine Sicherheitslücke dar.

Eine weitere Auseinandersetzung mit dem Datenschutz in Blackboard findet in [Los06] statt. Zum Zweck einer Vorabkontrolle zum Datenschutz werden dabei konkrete Problembereiche des Systems vorgestellt, die die Informationelle Selbstbestimmung beziehungsweise den Datenschutz gefährden könnten. Vorabkontrolle bedeutet dabei, dass eine Untersuchung durchgeführt wird, die überprüft, ob und in welchem Maß geltende Datenschutzgesetze berücksichtigt werden. Eine Vorabkontrolle wird meist vor dem regulären Einsatz der zu prüfenden Software vorgenommen.
Als Problembereich wird von Loser beispielsweise die Zeitstempel von Beiträgen in Diskussionsforen von Blackboard genannt [Los06]. Dadurch ist eine Verhaltenskontrolle der Benutzer möglich und deren Arbeitszeiten innerhalb der Lernplattform werden transparent. Des Weiteren werden von der Lernplattform Abruf- und Schreibereignisse zusammen mit dem entsprechenden Benutzer, dem Objekt und dem Zeitpunkt aufgezeichnet. Dabei sind diese Statistiken benutzerbezogen einsehbar.

Vorabkontrolle von Blackboard hat als Ziel, die von Loser genannten Problembereiche zu beheben und Blackboard datenschutzfreundlicher zu gestalten.

Zusammenfassung

Da Blackboard nicht für einen Direkttest zur Verfügung stand, ist eine Bewertung des Datenschutzes nur anhand der Fragebogenantworten und der angegebenen weiteren Quellen möglich.
Positiv hervorzuheben ist bei Blackboard die Möglichkeit, die Datenübertragung mittels SSL durchzuführen. Dies wird im Fragebogen und auch von [Cha03] genannt. Außerdem erhalten die Benutzer die Möglichkeit, die Preisgabe von personenbezogenen Daten zu konfigurieren, was eine wichtige Unterstützung der Informationellen Selbstbestimmung darstellt. Dies wird sowohl bei der Befragung und von Chan et al. [Cha03] angegeben als auch im Praxistest ermittelt.
Die von Loser vorgestellten Problembereiche geben die Sichtweise eines Datenschutzbeauftragten auf Datenschutzprobleme in Blackboard wieder [Los06]. Benutzerbezogene Statistiken und Forumsbeiträge, die durch Blackboard erstellt werden, sind nach Loser als nicht zweckgebunden einzustufen und geben die Möglichkeit einer übermäßigen Überwachung des Lernenden [Los06]. Sie sollten somit nur pseudonym festgehalten werden. Es konnte nicht ermittelt werden, ob dem Benutzer das Recht eingeräumt wird, Statistiken über ihn selbst mit einzusehen. Durch diese Option könnte der Benutzer stärker für das Thema Datenschutz sensibilisiert werden und somit besser beurteilen, welche Informationen das Lernmanagement-System über ihn erhebt und andere Benutzer über ihn einsehen können.

6.2.2 CLIX

Fragebogenantworten

Die für die Beantwortung zugrunde liegende Installation von CLIX verwendet CLIX Campus 5 und wird an der Universität des Saarlandes eingesetzt. Etwa 22000 Benutzer sind bei dieser Installation angemeldet. Der Fragebogen wurde von einem Administrator der dortigen CLIX-Installation beantwortet.

Datensparsamkeit: Eine pseudonyme beziehungsweise anonyme Benutzung der Lernplattform ist nicht vorgesehen. Aber nach Ansicht des Befragten werden keine personenbezogenen Daten gesammelt, die nicht für die Diensterbringung erforderlich sind. Außerdem wird auch auf die Weiterverarbeitung von Verkehrsdaten verzichtet.

Zweckbestimmung und Nutzungsbegrenzung: Der Zweck, für den Daten erfasst werden, ist vor der eigentlichen Datenerhebung festgelegt. Weiterhin kann durch das Lernmanagement-System gewährleistet werden, dass nur berechtigte Personen Zugriff auf personenbezogene Daten anderer Benutzer haben. Die Löschung von personenbezogenen Daten ist nicht vorgesehen und es liegt im Ermessen des Kursleiters, ob Foren- und Chatbeträge gelöscht werden.

Rollen und Zugriffsrechte: Es werden unterschiedliche Rollen angeboten und deren Rechte und Verpflichtungen werden durch das Lernmanagement-System sichergestellt. Diese Rollen werden nur durch Personen vergeben, die entsprechend autorisiert sind.

Rechte des Betroffenen und Informationelle Selbstbestimmung: Der Benutzer hat die Möglichkeit, seine eigenen persönlichen Daten direkt in der Lernplattform einzusehen und diese

zu modifizieren. Benutzeraktivitäten, die aufgezeichnet werden, kann ein Lernender nicht in dem Lernmanagement-System einsehen. Der Benutzer kann nicht mitentscheiden, welche persönlichen Daten über ihn gesammelt werden, für welchen Zweck diese verwendet werden und welche Benutzergruppen Zugriff auf die Daten haben dürfen. Auch erhält er keine Informationen darüber, wer Einsicht in seine personenbezogenen Daten genommen hat.
Eine Datenschutzerklärung kann mittels des Lernmanagement-Systems angeboten werden. Diese wird in der angegebenen Installation während des Erstlogins präsentiert, bei dem auch die Einwilligung zur Datenverarbeitung eingeholt wird. Des Weiteren ist die Datenschutzerklärung immer unter den persönlichen Benutzereinstellungen einsehbar. Eine Zusicherung, dass diese Datenschutzerklärung auch eingehalten wird, bietet das Lernmanagement-System nicht.

Sicherheit und Datenqualität: Eine geschützte Datenübertragung wird bei jeder Übermittlung von personenbezogenen und sensiblen Daten durch CLIX sichergestellt. Die Datenhaltung ist gesichert möglich, wird aber nicht für alle personenbezogenen Daten eingesetzt. Die Sicherheitsmaßnahmen sind durch autorisierte Rollen global für alle Teilnehmer einstellbar.
Die Lernplattform bietet die Möglichkeit, Benutzer eindeutig mittels LDAP[1]-Authentifikation zu identifizieren.
Dass die Informationen, die über einen Benutzer gesammelt werden, sachlich richtig sind, kann nach Aussage des Befragten durch die Lernplattform gewährleistet werden.

Recherche weiterer Quellen

In [CLI07] wird die Version CLIX Campus 6.1 näher erläutert, um Studierende bei der Verwendung dieser Lernplattform anzuleiten. Daraus lässt sich entnehmen, dass die Benutzer der gesamten Lernplattform oder wahlweise die Teilnehmer der Vorlesungen und Communities, an denen ein Benutzer teilnimmt, eingesehen werden können. Dabei hat man in CLIX die Möglichkeit, das hinterlegte Profil der Benutzer, deren Online/Offline-Status und das Gästebuch einzusehen sowie dem entsprechenden Benutzer eine eMail zu senden. Aus [CLI] ist außerdem ersichtlich, dass ein Protokoll aller Foreneinträge oder Chatnachrichten des aktuellen Forums oder Chats durch jeden Benutzer, der berechtigt ist darauf zuzugreifen, gespeichert werden kann. Bei der Wiederverwendung einer Vorlesung wird in CLIX 5.0 gewährleistet, dass weder Teilnehmerlisten aus vergangenen Semestern noch Einträge aus Foren und Chats übernommen werden [CLI05].

Aus einer Bewertung von CLIX 3.0 [CLI01] können weitere Informationen entnommen werden. CLIX besitzt ein sehr flexibles Rollenkonzept, durch das sich beliebig viele Rollen definieren lassen. Diese Rollen können mit individuellen Rechten versehenen werden. Auch können Rechte und Sichtbarkeiten bestimmter Elemente in CLIX auf Basis von Katalogen, Benutzergruppen sowie einzelnen Benutzern vergeben werden.
In [CLI01] fand auch eine Bewertung der Sicherheitstechnologien statt. So wird eine verschlüsselte Übertragung per SSL vollständig unterstützt. Jedoch wird der Schutz personenbezogener Daten nur teilweise erfüllt, was der Autor damit begründet, dass der Datenschutz von der jeweiligen Kombination und Vergabe der Nutzerrechte abhängig ist. CLIX verwendet ein *Learning Data Tracking*, bei dem das Navigationsverhalten, die Verweildauer in Kurselementen, der Lernfortschritt und die Testergebnisse der Benutzer wiedergegeben und statistisch ausgewertet werden können.

[1] Lightweight Directory Access Protocol

Zusammenfassung

CLIX konnte zwar nicht anhand eines Praxistests, aber durch Befragung und Hinzunahme weiterer Quellen bewertet werden. Bei der Installation, die für die Befragung zur Verfügung stand, ist die feste Integration der Datenschutzerklärung und des Einwilligungsprozesses positiv hervorzuheben. Das Lernmanagement-System unterstützt die Vergabe von Rollen und Rechten. Allerdings ist laut [CLI01] eine sehr feingranulare und weit reichende Rechtevergabe möglich, so dass der Datenschutz nur bei sehr gewissenhafter Vergabe von Rechten gewährleistet werden kann.

6.2.3 WebCT

Fragebogenantworten

Die Installation von WebCT, die für die Befragung zu Grunde lag, wird vom Sächsischen Bildungsserver betrieben. Es handelte sich um WebCT 4.1.5.8 Campus Edition mit einem Lizenzmodell, das auf einer maximalen Teilnehmeranzahl von 3000 basiert. Zum Zeitpunkt der Untersuchung waren etwa 1000 Benutzer bei dieser WebCT-Installation registriert. Das Lernmanagement-System wird zur Unterstützung der Lehre an sächsischen Hochschulen und Schulen eingesetzt. Zur Beantwortung des Fragebogens stand ein Administrator der WebCT-Installation zur Verfügung.

Datensparsamkeit: Der Benutzer ist immer mit einer nicht wechselnden, eindeutigen Benutzer-ID angemeldet und kann die Lernplattform somit weder anonym, noch unter mehreren Pseudonymen verwenden. WebCT speichert die Aktivitäten, die ein Lernender in einem Kurs durchführt. Dabei werden das erstmalige und das letztmalige Betreten des Kurses gespeichert. Des Weiteren wird festgehalten, welche Inhaltskategorien wie oft durch den Lernenden aufgerufen wurden und wie viele Beiträge in den Foren gelesen und geschrieben wurden. Bei Inhaltsseiten kann betrachtet werden, welche Seiten der Lernstoffpräsentation zu welchem Zeitpunkt durch den Lernenden aufgerufen wurden. Dabei wird minutengenau dokumentiert, so dass der Lehrende auf die jeweilige Dauer einer Seitenbetrachtung schließen kann.

Zweckbestimmung und Nutzungsbegrenzung: Der Zweck der Datenverarbeitung ist vor der Erhebung festgelegt. Auch erhalten nur die Personen Zugriff auf die persönlichen Informationen und die Aktivitätsdaten der jeweiligen Kursteilnehmer, die laut Rollenkonzept dazu berechtigt sind.
Benutzer werden aus der Lernplattform gelöscht, wenn sie über sechs Wochen nicht auf die Lernplattform zugreifen. Dabei werden auch ihre persönlichen Daten, Aktivitätsdaten und Nachrichten aus den Kursen gelöscht.

Rollen und Zugriffsrechte: WebCT stellt vorgefertigte Rollen zur Verfügung, bei denen die Zugriffsrechte, die Berechtigungen zur Erstellung und Modifizierung von Inhalten und die Interaktionen mit anderen Teilnehmern vordefiniert sind. Rollen und damit verbundene Rechte können nur durch autorisierte Benutzer (den Administratoren) vergeben werden. Das Lernmanagement-System macht den Beteiligten aber nicht transparent, welche Rollen welche personenbezogenen Informationen einsehen können.

Rechte des Betroffenen und Informationelle Selbstbestimmung: In der untersuchten Installation von WebCT ist keine direkte Anmeldung möglich, sondern das Login wird schriftlich beantragt. Somit ist auch die Einwilligung zur Verarbeitung der personenbezogenen Daten

vorher schriftlich zu geben. Bei Jugendlichen unter 18 Jahren ist der Datenverarbeitung durch die Erziehungsberechtigten zuzustimmen. Die Einwilligung kann jederzeit durch eine eMail oder einen Brief an den Anbieter widerrufen werden. Einwilligung und deren Widerruf sind somit nicht in das Lernprogramm integriert. Ob durch die Lernplattform die Integration einer Datenschutzerklärung und den dazugehörigen Funktionen konkret unterstützt wird, kann somit nicht geprüft werden.
Durch die Lernplattform ist es nicht vorgesehen, dem Lernenden zu ermöglichen, selbst darüber zu entscheiden, welche Informationen über ihn gesammelt werden und auch der Zweck der gesammelten Informationen ist nicht konfigurierbar. Wer Zugriff auf personenbezogene Daten erhält, ist durch die Rechtevergabe des Lernmanagement-Systems festgelegt. So können der Kursleiter und der Administrator jederzeit auf Aktivitätsdaten und persönliche Daten eines Kursteilnehmers zugreifen.
Wann oder wie oft der Kursleiter die Daten eines Lernenden eingesehen hat, wird vom Lernmanagement-System nicht gespeichert und somit kann ein Kursteilnehmer diese Information auch nicht abrufen.

Sicherheit und Datenqualität: Die Lernplattform unterstützt die Verwendung von SSL zur Verschlüsselung der Übertragung. Dabei kann gewählt werden, ob nur die Anmeldung verschlüsselt wird oder der gesamte Datentransfer. Eine Konfiguration ist nur durch den Administrator möglich, der dies global für alle Teilnehmer der Lernumgebung vornimmt.
Alle Daten, die in der Lernumgebung erzeugt werden (einschließlich persönlicher Informationen), werden serverseitig gespeichert. Durch feste Zugriffsrechte können innerhalb der Lernplattform nur autorisierte Personen darauf zugreifen.
Durch die Vergabe von Zugriffsrechten sind eine unbefugte Einsicht, Modifikation und Löschung von Daten nicht möglich. Die Passwörter, die zur Authentifikation verwendet werden, können durch den Administrator in der maximalen und minimalen Länge festgelegt werden. Das Erstpasswort eines jeden Benutzers wird vom Administrator festgelegt und bei der ersten Verwendung der Lernplattform durch den eigentlichen Benutzer geändert.

Praxistest

Die vorgestellte Installation von WebCT wurde in der Rolle eines Kursteilnehmers sowie in der eines Kursleiters getestet. Dabei sind weitere Beobachtungen gemacht worden, die im Folgenden skizziert werden.

Es wird eine WebCT-interne eMail-Adressliste angeboten, in der die Kursteilnehmer und Kursleiter eingesehen werden können. Ob die Einsichtnahme möglich ist, wird vom Administrator festgelegt.
Die Kursteilnehmer und Kursleiter haben die Möglichkeit, auf einen Forumseintrag öffentlich und für alle sichtbar zu antworten, oder per eMail direkt demjenigen zu antworten, auf dessen Eintrag sie reagieren.
Ob der Lernende seine persönlichen Informationen und Aktivitätsdaten einsehen kann, ist von der Konfiguration des Kurses durch den verantwortlichen Kursleiter abhängig. Eine Modifikation von persönlichen Informationen über den Lernenden ist nur dem Administrator und dem Kursleiter im vollen Umfang möglich. In Abbildung 6.2 wird gezeigt, welche persönlichen Informationen eines Lernenden – dies sind die Spalten, die mit „Bearbeiten“ gekennzeichnet sind – durch den Kursleiter verändert werden können.

Abbildung 6.2: Bearbeitung persönlicher Informationen eines Lernenden durch den Kursleiter in WebCT

Der Lernende ist in der untersuchten Installation von WebCT nur berechtigt seine externe eMail-Adresse und sein Passwort verändern. Jedoch hat auch der Kursleiter das Recht, die Passwörter seiner Kursteilnehmer zu ändern.
Neben den in Abbildung 6.2 ersichtlichen Informationen über den Lernenden, speichert WebCT auch Aktivitätsdaten über den Lernenden, die Auskunft darüber geben, welche Inhaltsseiten er wie oft in einem Kurs besucht hat. Die Übersicht, die dabei durch den Kursleiter eingesehen werden kann, wird in Abbildung 6.3 dargestellt.
Bei Chaträumen wird darauf hingewiesen, dass die Kommunikation in diesen aufgezeichnet wird. Wie lange sie gespeichert werden, oder wer sie nach der Aufzeichnung einsehen kann, ist nicht beschrieben.

Homepage > Wie weit bin ich?
Kursteilnehmerprofil
Ganzer Name: Anne-Katrin Stange-Schüler
Benutzer-ID: tud_stanges
Erstes Einloggen: Juni 21, 2007 15:56
Letztes Einloggen: Juli 9, 2007 16:40
Gesamtanzahl der Zugänge: 19
Zuletzt besuchte Seite: Positionieren von Elementen
Historie der Inhaltsseiten besucht von Anne-Katrin Stange-Schüler (tud_stanges)
Verteilung der Besucher anzeigen
Objekte 2-11 von 11
Seitenname
Zugangszeit
11 Positionieren von Elementen Juli 9, 2007 16:40
10 Wichtige Attribute Juli 9, 2007 16:40
9 Hinweise Juli 9, 2007 16:40
8 Umgang mit Tags Juli 9, 2007 16:40
7 Hilfsprogramme Juli 9, 2007 16:40
6 Einführung Juli 9, 2007 16:40
5 Hinweise Juli 9, 2007 16:40
4 Hinweise Juli 9, 2007 16:39
3 Hinweise Juli 9, 2007 16:39
2 Einführungstest Juli 9, 2007 16:35

Abbildung 6.3: Historie der Inhaltsseiten, die ein Lernender in einem Kurs betrachtet hat (WebCT)

Nach der Bearbeitung eines Tests durch den Lernenden kann der Kursleiter auf die Fertigstellung der Aufgabe durch die automatische Zusendung einer eMail hingewiesen werden. Dies wird dem Lernenden vor Absenden der Aufgabe sichtbar gemacht.
Der Administrator kann festlegen, ob und in welcher Art und Weise andere Kursteilnehmer sichtbar sind. Wenn sie für die anderen sichtbar sind, kann dies auf Grundlage des Namens, der Benutzer-ID oder beidem geschehen. Außerdem kann der Administrator festlegen, ob und wie oft ein Benutzer sein Passwort verändern muss.

Recherche weiterer Quellen

In [Cha03] wird WebCT in Bezug auf dessen Sicherheitsmechanismen und der Unterstützung der Privatheit der Benutzer folgendermaßen charakterisiert:

- Authentifikation: proprietäre ticket-basierte und browser-basierte Authentifizierung, sowie Single Sign-On;
- Zugriffskontrolle: rollen-basierte Autorisierung;
- Vertraulichkeit: ausgewählte Daten sind mittels SSL verschlüsselt;
- Integrität: keine Unterstützung von digitalen Signaturen;
- Nachweisbarkeit: beruht auf der Speicherung von Aktivitätsdaten;
- Privatheit: Leistungen der Lernenden und der Zugriff auf Kursseiten sind nicht anonym. Die Lernenden haben keine Möglichkeit ihre eigenen Informationen zu kontrollieren. So sind Lernende und Lehrende auch nicht berechtigt, ihre eigenen Profile zu verändern.

Aufgezeichnete Konversationen aus Chaträumen sind für den Kursleiter einsehbar und können von diesem für alle Kursteilnehmer sichtbar platziert werden. Die Bereiche *MeineNoten* und *MeinFortschritt* sind nicht für andere Kursteilnehmer einsehbar, jedoch wiederum für den Kursleiter. Gleiches gilt auch für das eMail-Postfach der einzelnen Kursteilnehmer [WCTa].

Bei der Wiederverwendung eines Kurses bleiben einige Inhalte, wie beispielsweise Beiträge, die in das dazugehörige Diskussionsforum geschrieben wurden, erhalten [WCTb]. So liegt die Entscheidung, diese Informationen zu entfernen oder sie für neue Teilnehmer des Kurses zur Verfügung zu stellen, beim Kursleiter. Des Weiteren wird in [Sch05] wird angegeben, dass Rollen in WebCT 4 nicht frei definierbar sind und somit nur vordefinierte Rollen verwendet werden können.

Zusammenfassung

Durch die vordefinierten Rollen in WebCT sind die Verantwortlichkeiten und Rechte der einzelnen Rollen leicht zu erfassen. Die Funktionen, die Zugang zu und Modifikation von persönlichen Daten der Lernenden ermöglichen, liegen vollständig außerhalb des Einflussbereiches der Lernenden. Gleiches gilt auch für die Aktivitätsdaten der Lernenden.
So kann für WebCT im Allgemeinen festgestellt werden, dass der Lernende direkt keinen Einfluss auf die Informationen, die über ihn gesammelt werden, nehmen kann. Er erhält aber die Möglichkeit, wenn es durch den Kursleiter zur Verfügung gestellt wird, Einsicht in seine personenbezogenen Daten und auch in die Aktivitätsdaten zu nehmen.
Dass eine umfassende Löschung von personenbezogenen Daten eines Benutzers vorgenommen wird, wenn er die Lernplattform nicht mehr verwendet, kann neben dem Aspekt des Datenschutzes auch auf das Lizenzmodell zurückgeführt werden.

Aufgrund der weitreichenden Rechte der Rolle des Administrators und insbesondere auch des Kursleiters, sollten diese Verantwortlichkeiten mit großer Sorgfalt vergeben werden. So wird der Kursleiter beispielsweise in die Position versetzt, personenbezogene Daten und die Passwörter der Lernenden, die an seinem Kurs teilnehmen, zu ändern. Dadurch wird nicht nur der Zugriff auf den jeweiligen Kurs beeinflusst, sondern WebCT ist für einen Teilnehmer, der nicht in Kenntnis seines neuen Passworts versetzt wird, nicht mehr verwendbar. Somit erhält er auch keinen Zugriff mehr auf die Informationen, die in der Lernplattform über ihn gespeichert werden.

6.2.4 ILIAS

Praxistest

Für die eigene Untersuchung wurde die Demo-Installation[1] von ILIAS Version 3.7.9 verwendet, die von QUALITUS[2] zur Verfügung gestellt wird. Hier kann man an Kursen teilnehmen, die den Aufbau und die Funktionsweise von ILIAS erklären. Allerdings besitzt man nur die Rechte eines Lernenden und kann somit nicht alle Funktionen der Lernplattform testen.

Datensparsamkeit: Eine pseudonyme beziehungsweise anonyme Benutzung der Lernplattform ist nicht vorgesehen. Der Lernfortschritt wird entweder durch die Anzahl der Zugriffe oder durch die Dauer des Aufenthalts in einem Kurs berechnet. Ob weitere Informationen durch die Lernplattform über die Lernenden gesammelt werden, war bei dem Test nicht ersichtlich.

Rechte des Betroffenen und Informationelle Selbstbestimmung: Während der Registrierung bei ILIAS wird eine Nutzungsbestimmung angezeigt. Darin kann auch eine Datenschutzerklärung eingebettet werden. Bevor die Daten für die Registrierung übermittelt werden, muss der Nutzungsbestimmung zugestimmt werden, da ansonsten die Anmeldung nicht bearbeitet wird. Der Benutzer hat die Möglichkeit, seine eigenen persönlichen Daten, die er bei der Anmeldung angegeben hat, direkt in der Lernplattform einzusehen und diese zu modifizieren. Einige der Angaben sind als Pflichtangaben bei der Registrierung gekennzeichnet. Bei optionalen Angaben kann der Benutzer selbst entscheiden, welche weiteren Daten über ihn in der Lernumgebung gespeichert werden. Er kann aber nicht darüber entscheiden, für welchen Zweck diese verwendet werden sollen oder welche Benutzergruppen Zugriff darauf haben dürfen. Er kann ebenfalls nicht einsehen, welche anderen ILIAS-Benutzer Einblick in seine personenbezogenen Daten genommen haben. Die Informationen, die ein Benutzer über sich angegeben hat, kann er über eine Visitenkarte allen Benutzern der Lernplattform zugänglich machen. Dabei kann er für jede einzelne Information festlegen, ob sie öffentlich sein soll oder nicht (siehe Abbildung 6.4).

Recherche weiterer Quellen

Als Unterstützung für Anwender von ILIAS, werden mehrere Benutzerhandbücher online zur Verfügung gestellt [ILIb]. Aus diesen lassen sich weitere Informationen zu ILIAS entnehmen.

Datensparsamkeit: Die personenbezogenen Angaben, die im Profil des Benutzers enthalten sind und durch den Benutzer anderen zugänglich gemacht werden, können von allen Benut-

[1] http://www.demo.ilias-support.com/
[2] http://www.qualitus.de/de/1.html

zern als Visitenkarte herunter geladen werden. Dies können zum Beispiel Angaben zur Adresse, Telefonnummer, persönliches Bild, eMail und Interessen des Benutzers sein. Weitere Angaben, die von der Lernplattform erfasst werden, sind Angaben zur Häufigkeit und Dauer der Nutzung von Lernangeboten, sowie der letzte Zugriff. Anhand der Zugriffe oder der Zeit, die ein Lernender in einem Kurs verbracht hat, kann der Bearbeitungsstand einzelner Kurse angezeigt werden (Abbildung 6.5).

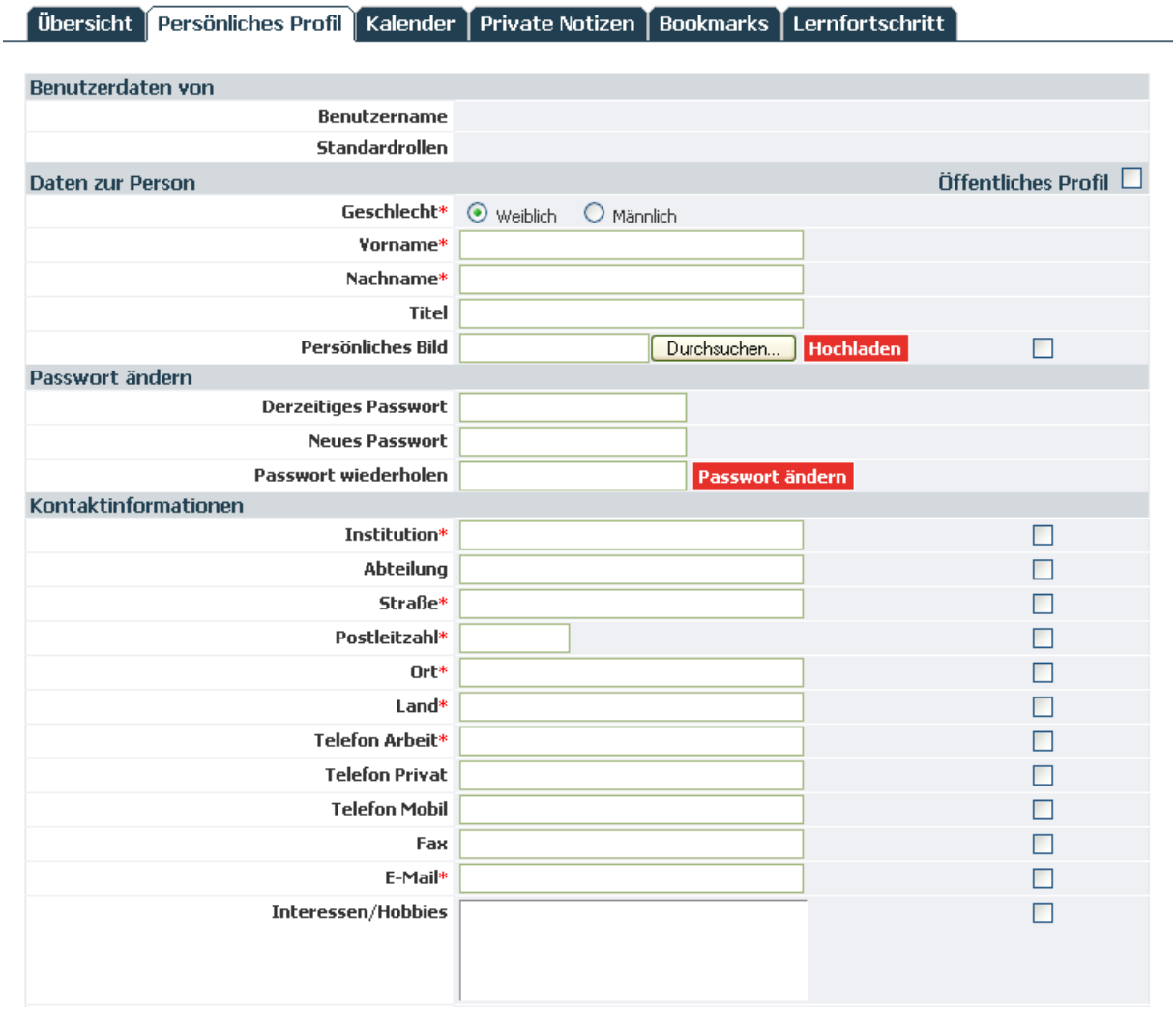

Abbildung 6.4: Anzeige des persönlichen Profils eines ILIAS-Benutzers

Der Administrator kann konfigurieren, welche Angaben bei der Registrierung Pflicht sind und welche optional beantwortet werden können. Außerdem kann er festlegen, dass einmal gemachte Angaben nicht mehr durch den Benutzer modifiziert werden dürfen.
In ILIAS besteht nach [ILIa] bei Umfragen und Tests die Möglichkeit, diese anonym durchzuführen. Vor der Teilnahme an einer Umfrage wird der Benutzer darauf hingewiesen, ob diese anonym durchgeführt wird oder nicht. Anonyme Tests sind zur Selbsteinschätzung des Lernenden gedacht und können nicht von dem Kursleiter eingesehen werden.

Abbildung 6.5: Anzeige des Lernfortschritts in ILIAS aus Sicht des Lernenden

Administratoren können von anderen Benutzern das Datum des letzten Logins und die Gesamtaufenthaltsdauer in der Lernplattform einsehen [ILIa].

Zweckbestimmung und Nutzungsbegrenzung: Ob der Zweck der Datenverarbeitung vor der Datenerhebung festgelegt ist, konnte im Rahmen der Untersuchung nicht geklärt werden. Jedoch wird durch das Lernmanagement-System gewährleistet, dass nur berechtigte Personen Zugriff auf personenbezogene Daten anderer Benutzer haben. Die Löschung von personenbezogenen Daten ist im System nicht vorgesehen, weshalb derartige Informationen bisher archiviert werden.
Durch die *Who-is-online*-Funktion kann eingesehen werden, welche Benutzer der Lernplattform gerade online sind. In den Benutzereinstellungen kann jeder Benutzer entscheiden, ob er diese Funktion verwenden möchte. Auch kann er entscheiden, ob er nur Teilnehmer aus seinen Kursen und Gruppen angezeigt bekommen möchte oder alle Benutzer, die derzeit online sind. Diese Funktionalität beinhaltet jedoch nicht, dass Benutzer, die die Online-Anzeige abstellen, selbst nicht mehr gesehen werden. Der Administrator kann diese Funktionalität auch für alle Benutzer einheitlich vorgeben, so dass der einzelne Benutzer nicht mehr wählen kann.
Foreneinträge bleiben nach der Löschung eines Benutzer-Accounts bestehen, aber der Autor wird anonymisiert [ILIa].

Rollen und Zugriffsrechte: Das Rollenkonzept gliedert sich in globale und lokale Rollen. Dabei hat jeder Benutzer anfangs eine globale Rolle, die im ganzen System gültig ist. Dazu gehören unter anderem die Rollen Gast, Benutzer und Administrator. Außerdem kann er noch weitere Rollen erhalten, die nur in bestimmten Bereichen des Lernmanagement-Systems Gültigkeit besitzen, wie zum Beispiel in Lernkursen oder Foren.

Sicherheit und Datenqualität: Eine geschützte Datenübertragung wird bei jeder Übermittlung von personenbezogenen und sensiblen Daten sichergestellt. Die Sicherheitsmaßnahmen zur Übertragung sind durch autorisierte Rollen global für alle Teilnehmer einstellbar. Zur Authentifikation von Benutzern stehen Techniken wie LDAP und Shibboleth zur Verfügung.

Zusammenfassung

ILIAS konnte nicht auf Basis einer Befragung untersucht werden, da sich kein Ansprechpartner zur Verfügung gestellt hat. Aber ein Praxistest und die Recherche weiterer Quellen stellen ausreichend Informationen zur Verfügung, um ILIAS in die Bewertung einzubeziehen.
Eine sparsame Datenerhebung wird durch ILIAS unterstützt, so ist es dem Administrator möglich, selbst festzulegen, welche personenbezogenen Daten er von den Benutzern benötigt. Weiterhin kann er durch Konfiguration die *Who-is-Online* Funktion abstellen, wenn dies gewünscht wird. Soweit aus den Betrachtungen zu ILIAS entnommen werden kann, werden nur sehr wenige personenbezogene Aktivitätsdaten gespeichert, die darüber hinaus nur dafür genutzt werden, um den ungefähren Bearbeitungsstand des Lernenden anzuzeigen.
Auch bietet ILIAS teilweise die Möglichkeit, anonym Umfragen und Selbsttests auszufüllen.

Die *Who-is-Online* Funktion kann die Privatheit anderer beeinflussen, und es sollte die Möglichkeit geben, neben dem Ausblenden anderer aktiver Benutzer auch sich selbst bei bedarf auf unsichtbar zu stellen. Nur der Administrator ist bisher dazu berechtigt, für alle den Status diesbezüglich zu ändern.

6.2.5 Moodle

Fragebogenantworten

Die der Befragung zugrunde liegende Installation beinhaltet Moodle 1.5.2 und hat über 600 Benutzer. Zur Verfügung gestellt wird die Installation durch die Technische Universität Dresden. Für die Befragung stand der Administrator der vorgestellten Installation zur Verfügung.

Datensparsamkeit: Eine pseudonyme beziehungsweise anonyme Benutzung der Lernplattform ist nicht vorgesehen.

Zweckbestimmung und Nutzungsbegrenzung: Es kann durch das Lernmanagement-System gewährleistet werden, dass nur berechtigte Personen Zugriff auf personenbezogene Daten anderer Benutzer haben. Die Löschung von personenbezogenen Daten ist nicht vorgesehen und bisher werden personenbezogene Daten archiviert.

Rollen und Zugriffsrechte: Es werden unterschiedliche Rollen angeboten und deren Rechte und Verpflichtungen werden durch das LMS sichergestellt. Diese Rollen werden nur durch Personen vergeben, die entsprechend autorisiert sind.

Rechte der Betroffenen und Informationelle Selbstbestimmung: Der Benutzer hat die Möglichkeit, seine eigenen persönlichen Daten direkt in der Lernplattform einzusehen und diese zu modifizieren. Der Benutzer kann nicht mitentscheiden, welche persönlichen Daten über ihn gesammelt werden, für welchen Zweck sie verwendet werden sollen, welche Benutzergruppen Zugriff darauf haben dürfen und er kann nicht einsehen, wer Einblick in seine personenbezogenen Daten genommen hat.
Ob eine Datenschutzerklärung mittels des LMS angeboten werden kann, war bei der Befragung nicht ersichtlich, da bei der betrachteten Installation keine Datenschutzerklärung verwendet wird.

Sicherheit und Datenqualität: Eine geschützte Datenübertragung wird bei jeder Übermittlung von personenbezogenen und sensiblen Daten sichergestellt. Die Sicherheitsmaßnahmen zur Übertragung sind durch autorisierte Rollen global für alle Teilnehmer einstellbar. Die Informationen, die über einen Benutzer gespeichert werden, sind als sachlich richtig anzunehmen, da sie durch den Benutzer selbst eingegeben werden.
Die Lernplattform bietet die Möglichkeit, Benutzer eindeutig mittels aktueller Techniken zu identifizieren, insbesondere wird bei der zugrunde liegenden Installation eMail-Authentifikation verwendet.

Praxistest

Für einen Test von Moodle konnte die Demo der offiziellen Moodle Webseite[1] versendet werden. Dort erhält man die Möglichkeit, Moodle in den Rollen des Administrators, Lehrers und Schülers zu testen.

Abbildung 6.6: Rechtevergabe durch den Administrator in Moodle

Moodle unterstützt den Administrator bei der Zuweisung von Rechten und Rollen. Dabei kann aus vielen zahlreichen Rechten gewählt werden. Damit der Administrator die Auswirkungen der einzelnen Rechte einschätzen kann, sind diese mit Hinweisen über die Risiken versehen. So wird unter anderem auch angezeigt, wenn bestimmte Rechte es ermöglichen, auf private Informationen von anderen Benutzern zuzugreifen. Dies ist in Abbildung 6.6 dargestellt.
In Moodle werden bei Aktivitätsstatistiken auch die jeweiligen IP-Adressen der Benutzer angegeben, durch die es weiterhin möglich ist, sich den Standort dieser Benutzer anzeigen zulassen (siehe Abbildung 6.7). Dadurch ist eine anonyme Verwendung der Lernplattform nicht gegeben. Da auch bei einem Gast-Account dessen IP-Adresse angezeigt wird. Die Aktivitätsdaten beinhalten weiterhin den Kurs, die Zeit, den vollständigen Namen, die Aktion und welche Inhalte damit verknüpft sind. Diese Aktivitätsdaten können von Moodle unbegrenzt

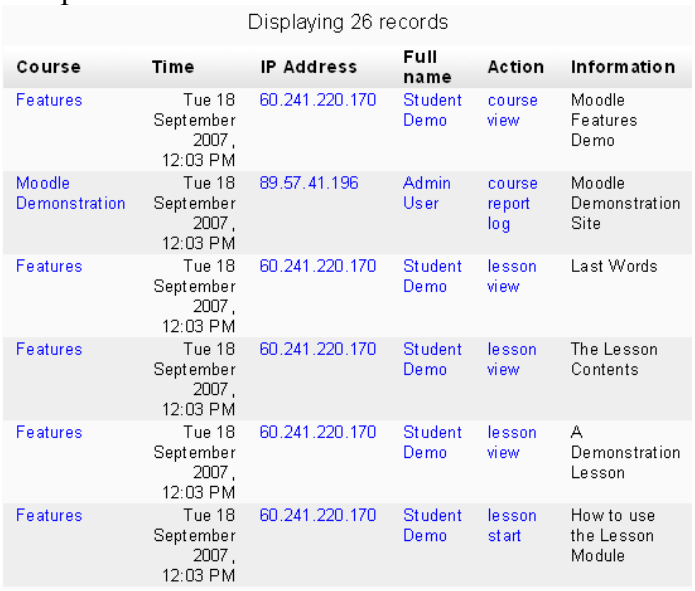

Abbildung 6.7: Anzeige der Beutzeraktivitäten in Moodle

[1] http://demo.moodle.org/

gespeichert werden.
Durch Moodle wird es ermöglicht, eine eigene Datenschutzerklärung in das System einzubinden.
Zur Authentifikation werden unter anderem LDAP und Shibboleth angeboten.
Verschlüsselung der Datenübermittlung mittels SSL wird zur Verfügung gestellt.

Recherche weiterer Quellen

Bei der Datenschutzuntersuchung von Moodle ist aufgefallen, dass eine rege Auseinandersetzung mit dem Thema Datenschutz in Moodle stattfindet. Dabei kommen die Anregungen von der Moodle-Community (siehe das deutsche Moodle-Forum), die für ihre jeweiligen Moodle-Installationen datenschutzrechtliche Maßnahmen wünschen oder benötigen [MDLa]. Daraus ist eine Arbeitsgruppe entstanden, die gegenwärtig mögliche Lösungen für eine datenschutzfreundliche Umsetzung von Moodle diskutiert. Das Ziel dieser Gruppe ist, konkrete Änderungen in der Software vorzunehmen, die den Datenschutz fördern, und anderen Moodle-Benutzern zur Verfügung zu stellen.

Problembereiche von Moodle hinsichtlich des Datenschutzes konkretisiert dabei beispielsweise Glameyer [Gla06]. In seiner Arbeit bezieht sich Glameyer auf die Moodle-Installation der FernUniversität Hagen, die studienbegleitend eingesetzt wird.
Nach Ansicht des Autors müssten folgende Aspekte den Benutzern verdeutlicht werden:

- Tutoren sind berechtigt, sich als beliebiger Benutzer ihres Kurses anzumelden und in dessen Namen zu handeln.
- Daten über das Verhalten der Benutzer werden gesammelt und jeder Tutor hat darauf Zugriff.
- Benutzerdaten werden bei einer Löschung des Benutzers nicht gelöscht, sondern nur ausgeblendet und können vom Administrator jederzeit wieder vollständig angezeigt werden.
- Jeder Tutor ist berechtigt, Kopien der Kursumgebung inklusive persönlicher Daten der Teilnehmer zu speichern und kann diese in jeder Moodle-Umgebung wieder herstellen.

Es wurde die Standardinstallation von Moodle 1.7 als Grundlage für die vorgestellten Überlegungen verwendet, die zwar schon Konfigurationsmöglichkeiten zu einigen der besprochenen Kritiken anbietet, diese aber standardmäßig nicht enthalten sind.
Unter anderem wurden in [Gla06] folgende Kritiken beziehungsweise Verbesserungsvorschläge präsentiert:

Die Datenschutzerklärung und Kontaktdaten sollten auf der Startseite angegeben werden und die Datenschutzerklärung sollte ebenfalls in das Anmeldeverfahren integriert werden.
Der Import und Export von Kursdaten wird auf den Administrator beschränkt, da ansonsten das Missbrauchsrisiko als zu hoch eingeschätzt wird und die zu schützenden Daten den Kontrollbereich der Verantwortlichen verlassen[Gla06].
Der Zeitraum, für den Protokolle von Chatkonversationen aufgezeichnet werden, soll vor dem Betreten des Chatraums für die Teilnehmer sichtbar sein.
Nur die BenutzerID wird beim Löschen eines Benutzers überschrieben. Informationen wie der Name, Kontaktdaten und die Personenbeschreibung bleiben aber erhalten.
Für die Unterstützung des selbstverantwortlichen Umgangs mit personenbezogenen Daten sollte die Profilseite durch Hinweistexte angepasst werden, so dass der Benutzer informiert wird, welche Konsequenzen die Angabe von personenbezogenen Informationen haben kann.

Moodle bietet die Funktion Login-As an, die es Administratoren und Lehrenden ermöglicht, sich mit der Identität eines Lernenden anzumelden und Aktionen auszuführen. Dies beeinträchtigt die Authentizität des Lernenden und ist nach Meinung des Autors nur für den technischen Support durch einen Administrator geeignet.

Eine Vielzahl von Aktivitäten der Moodle-Benutzer wird in einer Log-Datei gespeichert, die eine personalisierte statistische Auswertung ermöglichen. Der Autor schlägt hier vor, die Daten minütlich zu löschen, damit Auswertungen nicht möglich sind.
Der letzte Zugriff auf die Lernplattform ist durch Last-Access für jeden Kursteilnehmer mit Datum und Uhrzeit einsehbar. Dies könnte als Verletzung der Privatsphäre angesehen werden und Lernende könnten sich kontrolliert fühlen. Durch die Ersetzung der genauen Zeitangabe durch einen farblich gestalteten Balken könnte diese Problematik geändert werden.
Aus den in [Gla06] vorgestellten Problemen und dazugehörigen Lösungen kann man entnehmen, dass konkrete Anstrengungen unternommen werden, um den Datenschutz und insbesondere die Transparenz der Datenverarbeitung in Moodle zu erhöhen. Des Weiteren wird der Zugriff auf Funktionen, die ein Missbrauchsrisiko darstellen, nur noch Administrator zugänglich gemacht.

Zusammenfassung

Moodle ermöglicht durch das Aufzeichnen konkreter Benutzeraktivitäten und Verkehrsdaten, wie der IP-Adresse, eine sehr genaue Verfolgung der Aktivitäten und sogar des Benutzerstandortes.
Positiv sind bei Moodle, die Hinweise bei der Rollenerstellung hervorzuheben. Hier ist der Administrator durch die Hinweise zu den Risiken immer über die Datenschutzauswirkungen der einzelnen Rechte informiert, die er vergibt.

6.2.6 OLAT

Fragebogenantworten

Zur Bewertung wurde das System OPAL Version 2.1, das auf OLAT basiert, verwendet. Dieses wird von Bildungsportal Sachsen zur Unterstützung der Lehre sächsischer Universitäten verwendet. OPAL hat derzeit über 16000 angemeldete Benutzer. Der Fragebogen wurde von einem Administrator dieser Installation beantwortet.

Datensparsamkeit: Es ist keine pseudonyme Nutzung der Lernplattform möglich, aber durch den Gast-Account wird eine eingeschränkte, anonyme Verwendung des Lernmanagement-Systems angeboten.

Zweckbestimmung und Nutzungsbegrenzung: Der Zweck der Datensammlung wird vor der Erhebung festgelegt. Es erhalten innerhalb der Lernplattform nur Personen Zugriff auf personenbezogene Daten und Aktivitätsdaten, die diese direkt benötigen.
Die Löschung von personenbezogenen Daten ist derzeit noch nicht möglich. Das Löschen von Benutzern und eine Anonymisierung von Verlaufsdaten befinden sich derzeit in der Entwicklung.

Rollen und Zugriffsrechte: Es gibt ein differenziertes Rollensystem und die unterschiedlichen Rechte können durch das Lernmanagement-System technisch gewährleistet werden. Dabei werden die Rollen und Rechte nur durch autorisierte Personen vergeben. Ein angemeldeter Benutzer kann mehrere Rollen in unterschiedlichen Kursen einnehmen.

Rechte des Betroffenen und Informationelle Selbstbestimmung: Das Lernmanagement-System unterstützt den Vorgang der Einwilligung zur Datenverarbeitung durch den Benutzer sowie die Möglichkeit diese zu widerrufen. Außerdem wird der Benutzer bei einer Änderung der Konditionen benachrichtigt. Die Lernplattform unterstützt die Möglichkeit eine Datenschutzerklärung bereit zu stellen.
Personenbezogene Daten können direkt in der Lernplattform eingesehen werden. Benutzeraktivitäten, die das Lernmanagement-System aufzeichnet, können nicht direkt eingesehen werden, werden aber auf Anfrage vom Systembetreiber zur Verfügung gestellt.
Die Modifikation personenbezogener Daten ist nur für bestimmte Einträge möglich. So können beispielsweise persönliche Daten, die durch die Hochschule übermittelt werden, nicht abgeändert werden. Ein Benutzer kann weiterhin nicht festlegen, welche personenbezogenen Daten und Aktivitätsdaten über ihn gespeichert werden dürfen. Auch kann er den Zweck für den seine personenbezogenen Daten verwendet werden sollen, nicht konfigurieren. Welche seiner personenbezogenen Daten anderen Benutzergruppen angezeigt werden, kann er jedoch einstellen. Ob und wer seine personenbezogenen Daten eingesehen hat, wird durch das Lernmanagement-System nicht angezeigt.
Auf Auswirkungen, die einzelne Rollen und Rechte auf die Privatsphäre der anderen Benutzer haben können, wird nicht explizit angegeben. Es werden aber organisatorische Maßnahmen ergriffen, die die Schulung und Belehrung von Personen umfassen. So soll erreicht werden, dass Personen, die Rollen mit erweiterten Rechten innehaben, diese verantwortungsbewusst nutzen.

Sicherheit und Datenqualität: Die Betreiber von OPAL gewährleisten eine gesicherte SSL-verschlüsselte Übertragung bei jedem Datenaustausch und eine geschützte Datenhaltung aller sensiblen und personenbezogenen Daten. Dies wird aber nicht durch das Lernmanagement-System selbst zur Verfügung gestellt, sondern durch weitere technische und organisatorische Maßnahmen. Nur autorisierte Personen können dabei die Schutzmaßnahmen zur Übertragung und Speicherung global für die Lernplattform konfigurieren.
Authentifiziert werden die Benutzer in OPAL durch die Übernahme der Identitäten aus Hochschuldatenbanken mittels Shibboleth. In OLAT allgemein sind weitere Registrierungsmechanismen möglich.
Um den Sicherheitszustand des Systems zu protokollieren, werden Informationen, wie Login, Logout, das Aufrufen von Kursen und Tests aufgezeichnet. Dadurch können sicherheitsrelevante Ereignisse einem konkreten Benutzer zugeordnet werden.
Durch das Berechtigungskonzept von OPAL können nur autorisierte Personen personenbezogene Daten einsehen, modifizieren und löschen. Die Übernahme personenbezogener Daten von den jeweiligen Hochschulen gewährleistet, dass die Daten richtig und aktuell sind.

Eigene Beobachtungen

Für eine eingehende Betrachtung von OLAT wurde die Demo-Installation[1] der offiziellen OLAT-Homepage verwendet. Diese bietet für die drei Hauptrollen Administrator, Kursautor und Student einen Einblick in die OLAT Lernumgebung Version 5.1.2.

Datensparsamkeit: Zur Anmeldung im System sind ein Benutzername, der Vor- und Nachname, eine eMail-Adresse und die Angabe der Lehranstalt notwendig. Weitere Angaben, wie beispielsweise Geschlecht, Geburtsdatum, Telefonnummern und Anschrift können bei Bedarf durch den Benutzer ergänzt werden.

[1] http://demo.olat.org/demo/dmz/

Absolviert ein Lernender einen Test, wird dabei die Zeit festgehalten, wann er ihn begonnen und beendet hat, sowie die Dauer, die er zum Ausfüllen benötigte.
Der Kursbesitzer und weitere Benutzer, die Zugriff auf die Datenarchivierung erhalten, können Log-Files über die Teilnehmer des Kurses einsehen. Dabei bietet OLAT selbst keine graphische Darstellung der enthaltenen Benutzeraktivitäten an, sondern stellt unter anderem Text-Dateien zur Verfügung, die heruntergeladen und durch externe Programme ausgewertet werden können. OLAT nimmt eine strenge Trennung zwischen personalisierten Log-Files, die für die Aktivitäten der Kursautoren angelegt werden, und anonymisierten Log-Files, die das Verhalten der Lernenden innerhalb des Kurses wiedergeben, vor (siehe dazu Abbildung 6.8). Bei den anonymisierten Log-Files werden für die einzelnen Benutzer zufällige Zahlenfolgen vergeben, die ihnen bei jeder Verwendung des Kurses wieder zugeordnet werden. Durch diese Unterteilung der Log-Files ist es den Autoren und Administratoren möglich, das Verhalten von gleichberechtigten Benutzern nachzuvollziehen. Das Verhalten der Lernenden kann durch die Vergabe von Pseudonymen zur Analyse der Nutzung der Kursinhalte hinzugezogen werden und identifiziert die Lernenden nicht. Eine personalisierte Statistik eines Lernenden kann dadurch für den Lehrenden nicht realisiert werden.

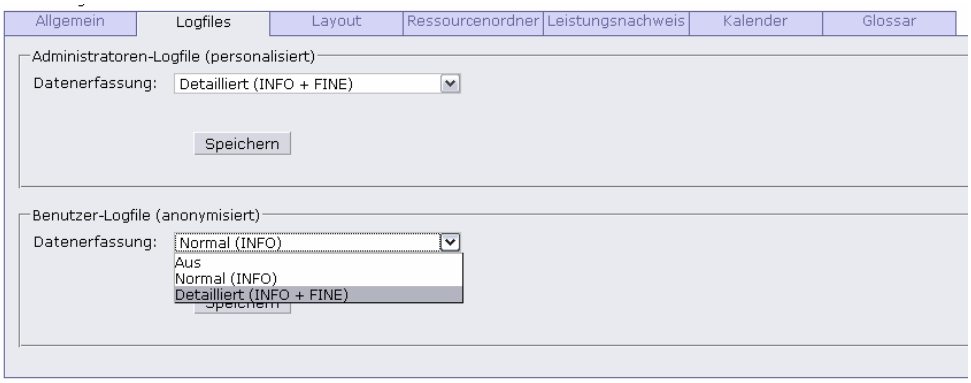

Abbildung 6.8: Konfiguration der Log-Files in OLAT

Den Detaillierungsgrad der Aufzeichnung des Benutzerverhaltens kann der Kursbesitzer für Autoren und Lernende jeweils getrennt konfigurieren. So sind bei einem niedrigen Detailgrad nur Aktionen der Benutzer sichtbar, aber nicht die Objekte oder Kursbestandteile, auf die sich diese Aktion bezieht. Dies kann aber in der detaillierten Darstellung eingesehen werden. Außerdem enthalten die Log-Files sekundengenaue Zeitangaben zu den Aktionen. Es wird dem Kursbesitzer aber auch angeboten, Log-Files vollständig zu deaktivieren.
Der Gäste-Account kann, wenn er angeboten wird, für eine anonyme Nutzung des Lernmanagement-Systems verwendet werden. Damit erhält man aber nur einen sehr eingeschränkten Zugriff auf Lernmaterialien, die ausdrücklich für Gäste freigegeben sind.

Zweckbestimmung und Nutzungsbegrenzung: Angaben, die im Benutzerprofil gemacht werden, können von Benutzern mit höheren Rechten, wie Autoren und Administratoren, gelesen werden.
Beim Kopieren eines Kurses werden Benutzerdaten, die in dem Kurs enthalten sind, nicht mitkopiert. Diskussionsthemen können durch den Kursbesitzer und andere Teilnehmer mit Archivierungsrechten gespeichert werden.

Rollen und Zugriffsrechte: OLAT stellt einerseits Systemrollen zur Verfügung, die in der gesamten Lernplattform gelten und ergänzt diese andererseits durch Lernrollen, die nur in jeweils einem einzelnen Kurs Auswirkungen haben. Der Kursbesitzer vergibt die Rechte an weitere Benutzer. Dabei können diese Zugriff auf das Gruppenmanagement, den Kurseditor, die Datenarchivierung und auf Bewertungswerkzeuge erhalten. Diese Rechte sind unabhängig

davon, welche Berechtigungen diejenigen innerhalb OLAT schon innehaben. So kann beispielsweise ein Lernender eine Tutoren-Rolle in einem Kurs einnehmen.

Rechte des Betroffenen und Informationelle Selbstbestimmung: Der Benutzer erhält bei einigen Funktionen der Lernplattform Hinweise, wer berechtigt ist, die Ergebnisse in personalisierter oder anonymisierter Form einzusehen. So werden Evaluationsergebnisse und Fragebogenantworten anonym gespeichert. Andere Testergebnisse stehen Administratoren und Autoren mit Personenbezug des Kurses zur Verfügung. In Selbsttests haben Betreuer weder personalisiert noch anonymisiert Einblick.
In OLAT wird jedem Benutzer die Möglichkeit gegeben, eine Visitenkarte über sich zu erstellen. Standardmäßig sind darin die BenutzerID und der Name enthalten. Der Benutzer kann aber darüber hinaus auswählen, welche weiteren personenbezogenen Informationen er den anderen OLAT-Benutzern über sich preisgeben will, und kann dies durch einen Text und ein persönliches Bild ergänzen. Visitenkarten können von allen Benutzern in OLAT eingesehen werden. Des Weiteren können die Inhalte der öffentlichen Ordner eines jeden Benutzers eingesehen werden sowie Kalendereinträge. Dabei kann jeder Benutzer selbst entscheiden, ob er Kalendereinträge öffentlich zugänglich macht, nur die jeweilige Zeit preisgibt oder ob er Kalendereinträge nicht sichtbar machen möchte.
Jeder Benutzer, unabhängig von seinen Rollen und Rechten hat dieselben Optionen bei der Bearbeitung seines Benutzerprofils.
Bei der Verwendung von Instant Messaging kann der Benutzer entscheiden, ob sein Online/Offline-Status angezeigt werden soll. Außerdem kann er, wenn er diese Statusanzeige zulässt, festlegen, ob andere einsehen dürfen, in welchem Kurs er zurzeit arbeitet und wie lange er schon online ist.
Bei der Archivierung von Log-Files erhält man einen Hinweis, dass die Nutzung der Inhalte der Log-Files nur für die Zwecke der Forschung und Lehre und für die Evaluation von universitären Belangen verwendet werden dürfen.

Zusammenfassung

Aktivitätsdaten von Lernenden werden in OLAT nur in anonymer Form festgehalten. Dies wird auf Grundlage der durchgeführten Untersuchung nur von OLAT angeboten. Auch dass Aktivitätsdaten von Lehrenden in personenbezogener Form gesammelt werden, stellt eine ganz neue Herangehensweise im Umgang mit Aktivitätsdaten dar. Die Möglichkeit des Deaktivierens dieser Funktionen ist ebenso gegeben und wird in den anderen Lernmanagement-Systemen bisher nicht angeboten.
Des Weiteren bietet OLAT auch die geeignete Platzierung einer Datenschutzerklärung an und ermöglicht die Veröffentlichung des eigenen Benutzerprofils.

6.2.7 BluES'n

Fragebogenantworten

Das Lernmanagement-System BluES'n wird an der Technischen Universität Dresden im Rahmen des EU-Projektes PRIME (Privacy and Identity Management for Europe) [PRI] entwickelt. Dabei wird insbesondere der Fokus auf die Entwicklung von Konzepten gelegt, die den Datenschutz und die Informationelle Selbstbestimmung im Lernkontext unterstützen können.

BluES'n besteht aus einem konventionellen Lernmanagementsystem mit der Bezeichnung BluES (BluEs like universal eEducation System), das durch die Integration einer privacy-enhancing (datenschutzfördernden) Komponente, der PRIME-Plattform, erweitert wird.
Die folgenden Angaben beruhen auf zwei ausgefüllten Fragebogen, die von Entwicklern des Lernmanagement-Systems ausgefüllt wurden.

Datensparsamkeit: Durch die Verwendung der PRIME-Komponente können Funktionen in dem Lernmanagement-System eingesetzt werden, die den Gebrauch und die Verwaltung von partiellen Identitäten ermöglichen. Eine partielle Identität setzt sich aus Informationen zusammen, die einen Benutzer in einem bestimmten Kontext repräsentieren.
So ermöglicht BluES'n es einem Benutzer beispielsweise, dass er seine partielle Identität wechselt, wenn er von einem Lernkurs (hier Workspace genannt) zu einem anderen übergeht oder auch nur eine neue Aktion innerhalb eines Kurses ausführt. Er kann diese partiellen Identitäten verwalten und bei Bedarf auch löschen.
Durch die Bereitstellung von partiellen Identitäten wird ein Benutzer in die Lage versetzt, die Lernplattform pseudonym zu verwenden, indem er nur Informationen über sich preisgibt, die ihn nicht vollständig identifizieren. Eine anonyme Verwendung der Lernplattform wird ebenfalls ermöglicht, indem partielle Identitäten für jeden Kontext gewechselt und nicht wieder verwendet werden. Aber durch Konfigurationen von autorisierten Rollen kann festgelegt werden, dass zur Teilnahme an einem Kurs nur eine bestimmte partielle Identität je Benutzer verwendet werden darf.

Zweckbestimmung und Nutzungsbegrenzung: Mit Hilfe von *Data Handling Policies* kann der Zweck für den personenbezogene Daten erhoben werden, überwacht und eingehalten werden.
Zur Durchsetzung von Datenschutzrichtlinien gibt es serverseitig Zugriffskontroll-Mechanismen, die sicherstellen, dass nur Personen oder Gruppen Zugriff auf bestimmte personenbezogene Informationen gewährt wird, die durch die Datenschutzerklärung dazu berechtigt sind.
Nachdem der Zweck, für den personenbezogene Daten verarbeitet wurden, nicht mehr gegeben ist, ist eine Löschung dieser Daten vorgesehen. Diskussionsbeiträge im Foren und Chatkonversationen werden persistent auf dem Server gespeichert. Da aber die Benutzer in BluES'n Pseudonyme verwenden, die ihrer realen Identität meist nicht zuzuordnen sind, sind diese Beiträge nicht direkt einer Person zuzuordnen.

Rollen und Zugriffsrechte: BluES'n greift als ein wichtiges Konzept die Raummetapher auf und stellt den Benutzern spezielle Räume (*Workspace* genannt) zur Verfügung. Grundsätzlich werden der private Raum (*Personal Workspace*) und der für andere zugängliche Raum (*Shared Workspace*) unterschieden. Jeder Benutzer kann neue *Shared Workspaces* erstellen und andere Benutzer einladen. Grundsätzlich haben in BluES'n alle Benutzer die gleichen Rechte. Erst wenn einer von ihnen einen *Shared Workspace* erstellt, können weitere Rechte vergeben werden. Dabei ist der Ersteller des *Workspaces* dazu berechtigt anderen Teilnehmern Rechte für seinen *Workspace* zuzuteilen.
Um einen Dienst des Lernmanagement-Systems nutzen zu können, kann es notwendig sein, dass der Benutzer bestimmte Informationen über sich preisgibt, wie beispielsweise sein Alter oder die Zugehörigkeit zu einer Universität. Damit nicht die Notwendigkeit besteht, Daten über sich preiszugeben, die eine Person vollständig identifizieren, kommen so genannte *Credentials* zum Einsatz. Dies sind entweder anonyme oder personengebundene Zertifikate, die über bestimmte Attribute des Benutzers Auskunft geben. Der Eigentümer eines *Credentials* braucht dieses nicht vollständig zur Legitimierung offen legen, sondern die Preisgabe einzelner Angaben über seine Attribute, ist als Beweis ausreichend.

Rechte des Betroffenen und Informationelle Selbstbestimmung: Beim Start von BluES'n wird dem Benutzer eine *Privacy Policy* angezeigt, die allgemeine Informationen zur Handhabung von personenbezogenen Daten enthält. Zusätzlich wird der Benutzer vor einer Übermittlung von personenbezogenen Daten informiert und kann entscheiden, ob er der Übermittlung zustimmt und diese Daten zur Verfügung stellt oder ob er die Anfrage ablehnt. Dies wird in Abbildung 6.9 dargestellt. Ein Widerruf zur Datenverarbeitung wird durch das Programm nicht angeboten, allerdings können Übermittlungen von personenbezogenen Daten zukünftig verweigert werden. Auskunft über die Informationen, die über ihn gespeichert sind, kann ein Benutzer direkt erhalten. Einerseits sind die Daten die lokal auf den PRIME- und BluES-Clients gespeichert werden einsehbar, andererseits werden auch die Informationen über den Benutzer auf dem Server, wie Pseudonyme, Forums-Beiträge und Chatnachrichten, angezeigt.
Die PRIME-Plattform stellt Methoden zur Verfügung, mit denen sich die Handhabung von persönlichen und identifizierbaren Informationen festlegen lassen. Mit den so genannten *Data Handling Policies* (DHP) kann auf Benutzerseite spezifiziert werden, wie ein Empfänger personenbezogene Daten zu handhaben hat. Dies beinhaltet den Zweck, für den die Daten verwendet werden dürfen, auf welche Art und Weise auf sie zugegriffen werden darf, welche Empfänger vorgesehen und welche Bedingungen einzuhalten sind. Außerdem bietet BluES'n eine Rechtekontrolle an, durch die personenbezogene Daten intern so verwaltet werden können, dass sie nur bestimmten Benutzergruppen zugänglich gemacht werden.
BluES'n unterstützt aber nicht, dass Benutzer einsehen können, ob und welche ihrer personenbezogenen Daten, die auf dem Server gespeichert sind, durch andere Benutzer eingesehen wurden. Aber bei der Preisgabe von personenbezogenen Daten, die clientseitig gehalten werden, werden Informationen per *Datatrack* gesammelt, die Auskunft darüber geben können, welche Daten der Benutzer in welchem Kontext anderen Pseudonymen über sich preisgegeben hat.

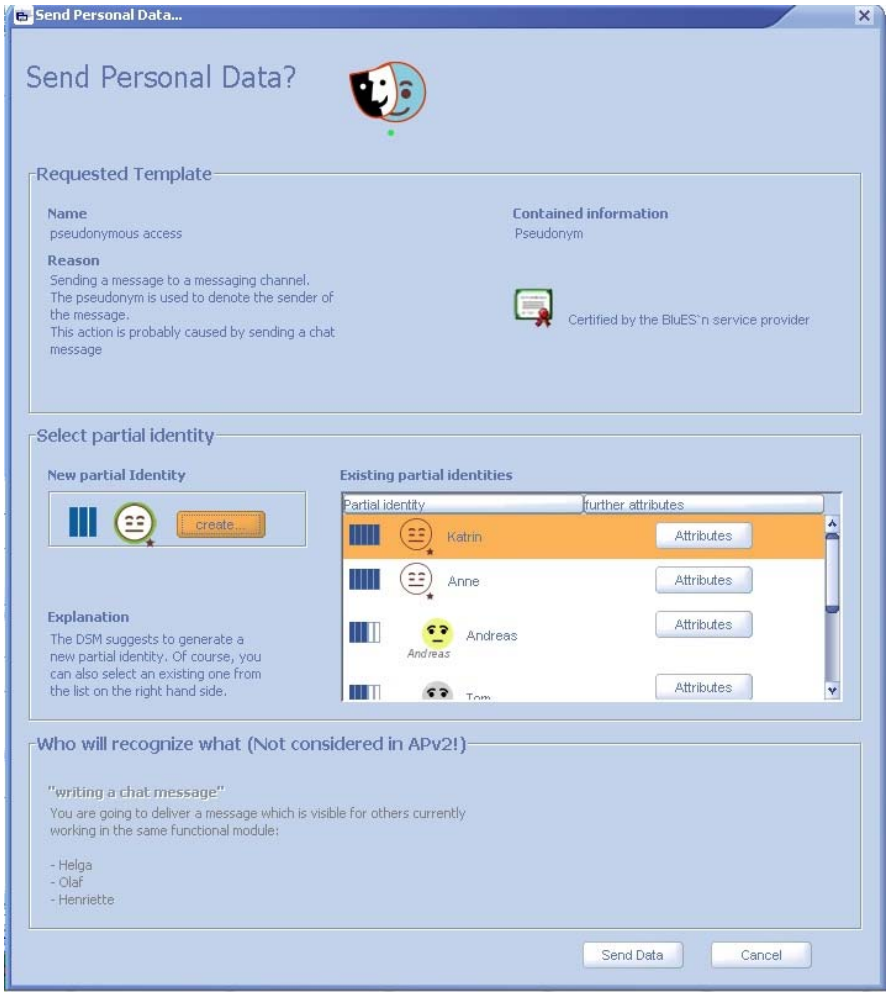

Abbildung 6.9 Dialog aus BluES'n, der anfragt, ob personenbezogene Daten übermittelt werden sollen

Sicherheit und Datenqualität: Eine geschützte Übermittlung von personenbezogenen Daten kann durch die Techniken der PRIME-Komponente realisiert werden. Dadurch wird jeder Benutzer in die Lage versetzt, selbst lokal Konfigurationen diesbezüglich vorzunehmen.
Personenbezogene Daten, die durch den Benutzer angegeben wurden, werden auf dessen PC unverschlüsselt gespeichert und durch ein Passwort geschützt. Andere Materialien die nicht personengebunden sind, wie Beiträge in Foren und Chaträumen, werden serverseitig gehalten. Bezüglich der gesicherten Datenhaltung muss der Benutzer für die auf seinem Computer gespeicherten Informationen weitere externe Sicherheitsmaßnahmen ergreifen, wenn er dies wünscht.
Im Normalfall können sicherheitsrelevante Ereignisse einem Pseudonym zugeordnet werden. Je nachdem welche Informationen ein Benutzer in einem Pseudonym über sich preisgibt, sind Rückschlüsse auf eine konkrete Person möglich.
Ein Schutz vor unbefugter Einsicht, Löschung und Modifikation ist durch die lokale Speicherung von personenbezogenen Daten dahingehend gewährleistet, dass Fremde keinen Zugriff auf diese Daten haben.
In BluES'n ist es möglich, die Echtheit von Benutzereigenschaften durch Zertifizierung sicherzustellen. Dafür wird das Zertifikat durch einen *Identity Provider*, der die Authentizität der Angaben bestätigt, ausgestellt. Damit die Echtheit der Angaben gewährleistet ist, sollte eine unabhängige Organisation die Stelle des *Identity Providers* einnehmen. Andererseits können unzertifizierte Eigenschaften verwendet werden. Diese gewährleisten aber keine Richtigkeit und Vollständigkeit der Angaben.

Recherche weiterer Quellen

Aus den Veröffentlichungen zu dem Framework [PRI06] und der Architektur [PRI07] der PRIME-Plattform lassen sich die Angaben aus den Fragebögen zu *Rechte des Betroffenen und Informationelle Selbstbestimmung* und *Sicherheit und Datenqualität* weiter spezifizieren.

Rechte des Betroffenen und Informationelle Selbstbestimmung: Durch den Einsatz des PRIME-Modules erhält der Benutzer die Kontrolle über seine personenbezogenen Daten und wird durch die Unterstützung der PRIME-Plattform in die Lage versetzt, sachkundig Entscheidungen über die Freigabe seiner Daten zutreffen. Auch nach einer Freigabe seiner personenbezogenen Daten kann der Benutzer Einfluss auf die Weiterverwendung dieser Informationen nehmen. So ist es vorgesehen, dass bei der Übertragung von personenbezogenen Daten auch Regeln übertragen werden, wie die Daten vom Empfänger verarbeitet werden dürfen [PRI07]. Nur wenn die Datenschutzpraktiken des Empfängers den Anforderungen des Eigentümers entsprechen, werden die Informationen übermittelt. Von der Bereitstellung der personenbezogenen Daten kann aber eine Diensterbringung abhängig gemacht werden, so dass der Eigentümer der Informationen entweder seine Anforderungen bezüglich des Datenschutzes anpasst, oder den Dienst nicht in Anspruch nehmen kann. Wurden die Datenschutzpräferenzen des Eigentümers akzeptiert, sind diese auch einzuhalten. Laut Konzept des Prototypen ist es geplant, dass der Eigentümer auch nach Freigabe seiner Daten noch Zugang zu diesen erhält, damit er sie einerseits aktualisieren und andererseits auch kontrollieren kann, ob die Anforderungen eingehalten werden [PRI07]. Außerdem kann der Benutzer selbst beziehungsweise weitere Institutionen durch die geeignete Verwendung von Trusted Computing-Technologien in die Lage versetzt werden, die Einhaltung von grundlegenden Sicherheits- und Vertrauenseigenschaften von entfernten Computersystemen eines Dienstanbieters zu überprüfen [PRI07].
Die schon vorgestellten *Data Handling Policies* (DHP) sind für den gesamten Zeitraum, für den der Anbieter auf die Daten zugreifen kann beziehungsweise sie aufbewahrt, gültig. Auf Seiten desjenigen, der die Informationen anfordert, kann mittels DHP angegeben werden, welche Datenschutzrichtlinien er unterstützt. Vergleichbar sind DHPs mit der P3P-Plattform, nur dass DHPs auch in durchsetzbare Richtlinien auf Seiten des Dienstanbieters umgewandelt werden können [PRI07]. P3P dient hingegen nur zum Austausch von Datenschutzerklärungen, um einem Internetanwender schnell und verständlich einen Überblick zu den Datenschutzpraktiken eines Dienstanbieters zu ermöglichen, ohne dass daraus eine Durchsetzung der Datenschutzrichtlinien resultiert (siehe auch Kapitel 5).
Des Weiteren wird ein *Privacy Obligation Management* eingesetzt, damit die Aspekte einer Datenschutzanforderung, die über Zugriffsberechtigungen von Daten hinausgehen, auch umgesetzt werden können [PRI07]. Darunter fällt zum Beispiel die Löschung von personenbezogenen Daten nach Wegfall der Erfordernis beziehungsweise zu einem festgelegten Zeitpunkt. Durch diese automatisierten Methoden, die die Umsetzung von Datenschutzanforderungen realisieren können, gestaltet es sich auch für Unternehmen einfacher, gesetzliche Datenschutzbestimmungen einzuhalten und mindert das Risiko, unabsichtlich dagegen zu verstoßen.
Nachdem der Benutzer für seine personenbezogenen Daten seine Datenschutzpräferenzen definiert hat, können auf Grundlage von regelbasierten Entscheidungen viele der nutzerseitigen Interaktionen, die die Weitergabe von personenbezogenen Informationen beinhalten, automatisiert werden.

Sicherheit und Datenqualität: Nutzerseitig ist geplant, dass das System einen Anonymisierungsdienst verwendet, durch den die Netzwerk-Adresse des Benutzers gegenüber dem jeweiligen Dienstanbieter verdeckt bleibt.

Die Benutzer agieren in der Lernplattform unter einem oder mehreren Pseudonymen. Unter bestimmten Bedingungen, beispielsweise wenn die Sicherheit des Systems verletzt worden ist oder um die Einhaltung von gesetzlichen Vorschriften zu garantieren, kann die Anonymität beziehungsweise Pseudonymität einzelner Personen jedoch aufgehoben werden.

Zusammenfassung

BluES'n wurde anhand von Befragungen und technischen Berichten des Frameworks und der Architektur bewertet. Ein Praxistest wurde nicht durchgeführt, da zum Zeitpunkt der Arbeit noch nicht alle benötigten Datenschutz-Mechanismen im Prototypen integriert waren.
Durch die Ergebnisse der Datenschutzbewertung ist ersichtlich, dass viele der aufgestellten Datenschutzkriterien durch BluES'n erfüllt werden können. Insbesondere sei hier nochmals auf die Möglichkeit hingewiesen, die Lernplattform anonym und pseudonym zu verwenden. Dabei können trotzdem Eigenschaften eines Benutzers durch die *Credentials* überprüft werden. Des Weiteren wird die Informationelle Selbstbestimmung durch zahlreiche Funktionen unterstützt. Der Benutzer erhält hier auch die Möglichkeit selbst festzulegen, ob er eine geschützte Datenübertragung zwischen sich und dem Dienstanbieter wünscht.

Im Gegensatz zu vielen anderen Lernplattformen ist BluES'n nicht browserbasiert, sondern setzt die Installation eines proprietären Clients voraus. Darüber hinaus werden alle personenbezogenen Daten, wie auch Zugangsberechtigungen, auf dem Computer gespeichert, auf dem BluES'n installiert wurde. Möchte ein Benutzer nun an verschiedenen Orten beziehungsweise auf verschiedenen Computern mit BluES'n arbeiten, müssen eine Reihe von Bedingungen erfüllt werden: Zum einen muss sichergestellt sein, dass auf den Computern, an denen der Benutzer arbeiten möchte, BluES'n installiert ist oder installiert werden kann. Zum anderen muss der Benutzer eventuell vorhandene, persönliche Daten mit sich führen, um überall die gleichen Rechte zu besitzen. Auch ist es Aufgabe des Benutzers für den Schutz der lokal gespeicherten Informationen zu sorgen und sie vor fremden Zugriff zu schützen.

Da BluES'n sich derzeit noch in der Entwicklung befindet und nur als Prototyp zur Verfügung steht, kann die Art und Weise, wie die vorgestellten Methoden und Konzepte hinsichtlich Transparenz und Offenheit umgesetzt wurden, noch nicht ausreichend beurteilt werden. Auch ist eine Bewertung hinsichtlich der Gebrauchstauglichkeit und Nutzerfreundlichkeit der Konzepte nicht möglich. Wie BluES'n die Anwender hinsichtlich deren Datenschutzbedürfnissen wirklich unterstützt und ob und welche Veränderungen sich im Vergleich zu anderen Lernumgebungen im Benutzerverhalten zeigen, sind Fragestellungen, die erst mit einer vollständigen Version geklärt werden können. Derzeit wird mit der Evaluation von BluES'n begonnen, dabei wird geprüft, ob die Umsetzung der Konzepte bei der Verwendung im Lernkontext verständlich sind und den Benutzer nicht überfordern.

6.2.8 Zusammenfassung

Die Bewertung der Lernmanagement-Systeme hinsichtlich des Datenschutzes zeigt, dass es Faktoren gibt, die bei der Vielzahl der Systeme vorhanden oder nicht vorhanden sind. Aber es zeigen sich auch Unterschiede in der Umsetzung einzelner Datenschutzaspekte auf.
So ist festzustellen, wenn man die Lernmanagement-Systeme bezüglich deren Zentrierung auf Lernenden oder Lehrende betrachtet, so wie es von Baumgartner vorgeschlagen wird (siehe Kapitel 2), dass dies auch den Datenschutz beeinflusst. Als Vertreter des lehrerzenrierten Ansatzes soll WebCT betrachtet werden, ILIAS als ein Vertreter des lernerzentrierten Ansatzes. Diese beiden Lernmanagement-Systeme sollen nun kurz gegenübergestellt werden.

WebCT, in der untersuchten Installation, gibt dem Lernenden wenige Möglichkeiten in die Hand, selbstständig in der Lernplattform zu agieren. Alles wird über den Lehrenden geregelt, der in WebCT dazu bevollmächtigt ist, die personenbezogenen Daten der Lernenden zu modifizieren und darüber entscheidet, ob ein Lernender seine Aktivitätsdaten und Noten einsehen darf. Dies wirkt sich natürlich auch auf die Informationelle Selbstbestimmung des Lernenden aus, die in WebCT nicht unterstützt wird. In ILIAS wird es hingegen dem Lernenden überlassen, neben den bereitgestellten Kursen, auch eigenständig in Communities zu lernen. Der Lernende kann sein Benutzerprofil jederzeit einsehen, bearbeiten und ergänzen. Außerdem kann er entscheiden, ob er die darin enthaltenen Informationen den anderen ILIAS-Benutzern anzeigen möchte. Auch der Lernfortschritt in den einzelnen Kursen ist für den Benutzer jederzeit einsehbar. In ILIAS wird dem Lernenden mehr Rechte zu gewiesen als in WebCT und die Informationelle Selbstbestimmung unterstützt.

6.3 Auswertung anhand der einzelnen Bewertungskriterien

Nachdem die Ergebnisse der Datenschutzbewertung für die einzelnen Lernmanagement-Systeme vorgestellt wurden, soll nun herausgearbeitet werden, wie gut die einzelnen Datenschutzkriterien von den Lernplattformen allgemein erfüllt wurden.

6.3.1 Datensparsamkeit

Bei der Betrachtung des Kriteriums der Datensparsamkeit ist auffällig, dass die Daten, die von einer Lernplattform gesammelt werden, nur geringfügig beeinflusst werden können. So wird schon bei der Entwicklung des jeweiligen Lernmanagement-Systems festgelegt, welche Daten über die Benutzer erfasst werden sollen und welche nicht. Insbesondere lässt sich die Erhebung von personenbezogenen Aktivitätsdaten nicht konfigurieren. Dies hat zur Folge, dass die Art und Menge der Informationen, die in den einzelnen Institutionen erforderlich sind und deshalb nur erhoben werden sollten, nicht mehr im System konfiguriert werden kann.
Eine anonyme Verwendung der in der Praxis eingesetzten Lernplattformen ist meist nur über Gastzugänge möglich, die aber keine Rechte zur eigentlichen Benutzung des Lernmanagement-Systems beinhalten. Die Unterstützung einer pseudonymen Verwendung der Lernplattformen, die an Universitäten zum Einsatz kommen, wird nicht bereitgestellt.
So ist es einem Benutzer nur in BluES'n möglich, pseudonym und anonym zu agieren.
Außerdem unterstützt BluES'n die Datensparsamkeit dadurch, dass nur Informationen über einen Benutzer preisgegeben werden, die wirklich für die Diensterbringung erforderlich sind.

6.3.2 Zweckbestimmung und Nutzungsbegrenzung

Aus den vorangestellten Ergebnissen kann man indirekt folgern, dass für den Zweck der Lehre genau die personenbezogenen Informationen erforderlich sind, die durch das Lernmanagement-System auch erhoben werden. Jedoch wird dieser Umstand in den seltensten Fällen kritisch hinterfragt. Setzt man sich mit der zweckgebundenen Datenerhebung genauer auseinander, erkennt man, dass die personenbezogenen Daten, die erhoben werden, für den eigentlichen Zweck oft zu genau sind und damit den Datenschutz verletzen (siehe dazu auch [Los06]). Weiterhin geben die Lernmanagement-Systeme meist den Umfang der Verarbeitung für personenbezogene Daten vor, indem sie den Anwendern nur bestimmte Funktionalitäten bereitstellen. Diese begrenzte Verarbeitung der Daten innerhalb der Lernplattform kann aber durch Exportfunktionen so umgangen werden, dass eine Gewährleistung der Nutzungsbegrenzung nicht mehr gegeben ist.

Außerdem wird die Handhabung von personenbezogenen Daten und Aktivitätsdaten nach Wegfall der Erfordernis meist nicht beachtet. So wird beispielsweise bei Moodle keine umfassende Löschung vorgenommen, sondern diese Informationen werden nur auf nicht sichtbar gestellt. Durch einen Administrator mit entsprechenden Rechten können diese Daten aber leicht wieder sichtbar gemacht werden.

6.3.3 Rollen und Zugriffsrechte

Die Vergabe von Rollen und Rechten wird in allen untersuchten Lernmanagement-Systemen nur von autorisierten Personen durchgeführt. Dabei werden globale Rollen und Rechte meist durch einen Administrator vergeben und lokale Rollen durch den Ersteller eines Kurses oder einer Gruppe. Diese werden auch in allen Lernplattformen technisch sichergestellt. Bei einigen der Lernmanagement-Systeme sind die Rollen und deren Rechte fest vordefiniert, bei anderen können auch eigene Rollen durch Kombination von Rechten erstellt werden.
Für die Beteiligten ist es dabei meist schwer ersichtlich, inwieweit Rollen und die damit verbundenen Rechte, Einfluss auf die Privatheit anderer Benutzer haben. Derjenige, der die Rechte innehat, merkt dies nur implizit durch die Ausübung seiner Rolle. Derjenige der Rollen und Rechte vergibt, wird nur in einigen Lernplattformen, wie beispielsweise bei Moodle, auf mögliche Konsequenzen hingewiesen. Aber der Benutzer, der durch die Rechte anderer in seiner Privatheit beeinflusst werden kann, wird am wenigsten über diesen Prozess aufgeklärt. In Moodle wird der Administrator bei der Zusammenstellung neuer Rollen durch Hinweise darauf aufmerksam gemacht, welche Rechte die Privatheit anderer Benutzer beeinflussen können. In anderen Lernmanagement-Systemen, wie OLAT oder ILIAS wird der Lernende teilweise informiert, welche Informationen und Testergebnisse über ihn durch andere Benutzer - wie Lehrende und Administratoren - eingesehen werden können. Bei der untersuchten Installation von WebCT ist der Lernende hingegen vom Lehrenden abhängig, wenn er überhaupt Informationen über sich und seinen Aktivitäten, die über ihn erhoben werden, einsehen möchte.

6.3.4 Rechte des Betroffenen und Informationelle Selbstbestimmung

Ob und wie gut eine Unterstützung des Einwilligungsprozesses zur Datenverarbeitung durch Lernmanagement-Systeme erfolgt, konnte durch die Untersuchung nur unzureichend ermittelt werden. Meist wird dies entweder außerhalb der Lernplattform angeboten, oder die allgemein angebotenen Werkzeuge des Lernmanagement-Systems werden für die Erstellung einer Datenschutzerklärung verwendet. In Moodle kann beispielsweise durch die Änderungen aus [Gla06] eine Datenschutzerklärung vor der eigentlichen Datenerhebung platziert werden und durch den Benutzer zugestimmt werden. Solch eine geeignete Platzierung der Datenschutzerklärung wird auch in ILIAS und CLIX angeboten.
Die eigene Einsichtnahme in persönliche Informationen des jeweiligen Benutzers wird in fast allen Lernplattformen ermöglicht. Dies unterstützt den Auskunftsanspruch des Betroffenen.
Weiterhin wird es aber nicht von allen Systemen realisiert, den Benutzer weitere Daten vollständig und jederzeit einsehbar darzustellen, die durch seine Interaktionen mit dem Lernmanagement-System entstehen und durch dieses aufgezeichnet werden. Ob eine Modifikation der eigenen personenbezogenen Daten durch den Benutzer erlaubt ist, kann von der Konfiguration des Benutzerprofils und von der Quelle der Daten abhängen.
Eine Überprüfung, ob die Datenschutzerklärung auch eingehalten wird, ist nach Aussage der Befragten nicht möglich. Dies ist für die Verbesserung des Datenschutzes noch zu realisieren

und könnte beispielsweise durch die von Yee et al. vorgestellte Technologie der *Secure Distributed Logs* umgesetzt werden.
Bei der Datenverarbeitung wird den Benutzern allgemein wenig Mitsprache gewährt. Die Erhebung von personenbezogenen Daten kann nur bei optionalen Daten beeinflusst werden. Der Zweck der Datenverarbeitung ist durch die Lernenden nicht beeinflussbar. So könnten sie beispielsweise festlegen, ob ihre Informationen für die Anzeige des Online-Status verwendet werden soll oder dass ihr Lernfortschritt nur pseudonym oder gar nicht für den Lehrenden einsehbar ist. Diese Funktionalitäten, wenn eine Konfiguration möglich ist, werden nur dem Kursleiter oder dem Administrator angeboten. Die Festlegung, welche Personen die eigenen personenbezogenen Informationen einsehen dürfen, wird dem Benutzer nicht überlassen. Meist wird nur zur Verfügung gestellt, ob die Informationen allen Benutzern der Lernplattform angezeigt werden sollen oder keinem. Aber eine bestimmte Auswahl an Benutzern, die diese Daten sehen dürfen, wird nicht angeboten. Auch die Möglichkeit einzusehen, welche Benutzer wann Informationen über einen Benutzer eingesehen haben, wird von keinem Lernmanagement-System angeboten.
Die in Kapitel 5 vorgestellten Spezifikationen IEEE PAPI und IMS LIP werden nach Aussage der Befragten nur von Blackboard unterstützt. Leider konnten keine anderen Quellen recherchiert werden, die genaue Angaben zur Unterstützung dieser datenschutzfreundlichen Spezifikationen für Lernmanagement-Systeme machen. Folglich ist keine sichere Aussage über die Richtigkeit dieser Information möglich.

Die Sensibilisierung der Benutzer ist ein sehr wichtiger Bereich des Datenschutzes, der besonders auf der organisatorischen Ebene unterstützt werden kann. Die untersuchten Lernmanagement-Systeme bieten dahingehend nur unzureichende Unterstützung. Der Benutzer wird zwar teilweise auf datenschutzrelevante Aspekte hingewiesen, dies wird jedoch nicht umfassend durchgeführt. So wird bei WebCT beispielsweise darauf hingewiesen, das Chatkonversationen gespeichert werden, aber nicht darüber informiert, für wen diese sichtbar sind und wie lange die vorgesehene Speicherdauer ist. Bei OLAT wird bei Umfragen und Tests informiert, ob diese anonym oder personenbezogen sind und wer berechtigt ist, diese einzusehen.

6.3.5 Sicherheit und Datenqualität

Die Datenübertragung zwischen der Lernplattform und einem Benutzer wird meist durch die Verwendung von SSL-Verschlüsselung realisiert. Dabei kann ein Lernmanagement-System selbst entsprechende Funktionen zur Verfügung stellen oder eine geschützte Übertragung wird durch externe Software umgesetzt.
Bei der Speicherung von personenbezogenen Daten wurde von einigen Befragten angegeben, dass es eine geschützte Datenhaltung gibt. Ob diese Funktionalität, wie bei BluES'n, direkt zur Lernplattform gehört oder auf eine externe Datenhaltung zurückgegriffen wird, ist dabei nicht erkennbar. Einige der Befragten gaben auch an, dass die geschützte Speicherung durch organisatorische Maßnahmen realisiert wird.
Häufig angegebene Methoden zur Authentifizierung werden mittels LDAP, Shibboleth und eMail-Registrierung durchgeführt. Eine Protokollierung zum Zweck den Sicherheitszustand zu überwachen, wird häufig nicht innerhalb der Lernplattform durchgeführt. Die in dem Lernmanagement-System protokollierten Aktivitätsdaten der Benutzer dienen in erster Linie dem Zweck der Lernfortschrittsverfolgung.
Ein Schutz vor unbefugter Löschung, Einsicht und Modifikation wird durch die Vergabe von Rechten realisiert. Dabei erhalten nur die Benutzer diesbezügliche Rechte, die sie mit Sorgfalt einsetzen. Dass die personenbezogenen Daten die Kriterien der Richtigkeit, Vollständigkeit und Aktualität erfüllen, wird meist durch die vertrauenswürdige Quelle, von der die Daten stammen, begründet. So liefert der Zugriff auf Studenteninformationen an Universitäten kor-

rekte Informationen, aber auch die direkte Eingabe der Daten durch den Benutzer kann als vertrauenswürdige Quelle angegeben werden.

6.4 Vergleich zur Studie „Privacy in eLearning“

Die Resultate der Datenschutzbewertung sollen nun mit den Ergebnissen der Umfrage „Privacy in eLearning“ [Sta06] verglichen werden. Die Umfrage „Privacy in eLearning“ wurde von Dezember 2005 bis Januar 2006 durchgeführt, wobei europaweit über hundert eLearning-Benutzer teilnahmen. Zu den Inhalten der Umfrage gehörten unter anderem Fragestellungen zu eLearning-Szenarien, in denen mögliche Funktionen einer eLearning-Umgebung vorgestellt wurden. Dabei hatten die Befragten die Möglichkeit, ihre individuelle Haltung zu diesen Funktionen durch Zustimmung oder Ablehnung wiederzugeben.

Die Funktionen, die in [Sta06] zu beurteilen waren, sind im Einzelnen:

1. Die Möglichkeit, in der eLearning-Umgebung anonym zu lernen,
2. Anlegen mehrerer Accounts oder Pseudonyme für unterschiedliche Lernbereiche und Inhalte,
3. Automatische Tutorbenachrichtigung bei schlechten Testergebnissen,
4. Mit einer einzigen Anmeldung beim Authentifizieren automatisch in allen weiteren Anwendungen und der eLearning-Umgebung eingeloggt zu werden,
5. Automatische Anpassung von Lerninhalten an das Vorwissen, die Berufsrichtung und den Bildungsabschluss,
6. Ansicht der persönlichen Daten und des Verlaufs, wer welche dieser Informationen einsehen darf,
7. Weitergabe von persönlichen Informationen ist nur mit Erlaubnis des Eigentümers.
8. Jeder ist berechtigt alles einzusehen.

In Abbildung 6.10 wird dargestellt, wie viel Prozent der Umfrageteilnehmer den gerade vorgestellten Funktionen 1. bis 8. etwas beziehungsweise sehr zugestimmt haben.

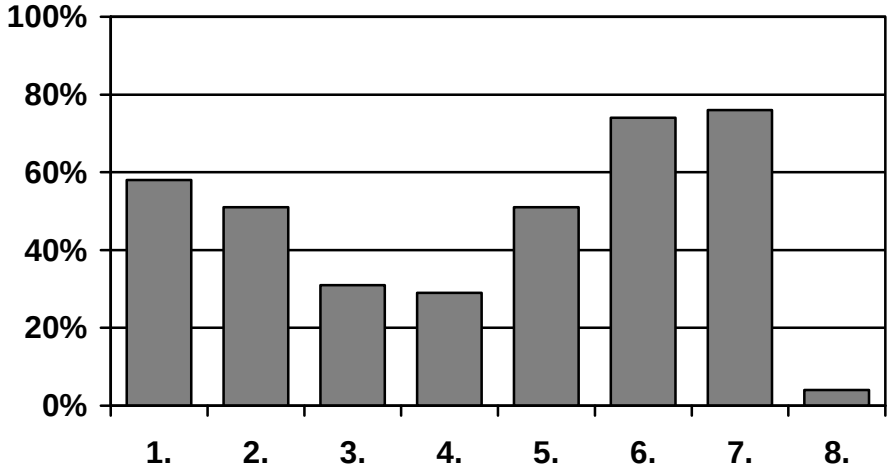

Abbildung 6.10: Prozentualer Anteil der Befragten, die den Funktionen 1. bis 8. sehr oder etwas zu stimmten

Die ersten beiden Funktionalitäten würden eine anonyme oder pseudonyme Benutzung eines eLearning-Systems ermöglichen. Dabei wurde die anonyme Verwendung von 58% und die

pseudonyme Verwendung von 51 % der Befragten befürwortet. Das bedeutet über die Hälfte der Umfrageteilnehmer wünschte sich eine solche Funktionalität im eLearning.
In der Datenschutzbewertung von Lernmanagement-Systemen sind die anonyme und pseudonyme Verwendung von Lernplattformen als Kriterien der Datensparsamkeit vertreten. Wie bei der Untersuchung der ausgewählten Lernmanagement-Systeme deutlich wurde, ist im Einsatz an Hochschulen keine anonyme oder pseudonyme Verwendung von Lernmanagement-Systemen vorgesehen. Es wird zwar in einigen Fällen ein Gastzugang angeboten, aber dieser verfügt nicht über die Berechtigungen, um auf Inhalte und Funktionen zuzugreifen. Als einziges Lernmanagement-System, dass auf eine pseudonyme Verwendung ausgelegt ist und auch eine anonyme Nutzung ermöglicht, ist BluES'n zu nennen.
Das bedeutet, auch wenn anonyme und pseudonyme Verwendung von eLearning-Systemen von den Umfrageteilnehmer befürwortet wurden und somit davon auszugehen ist, dass auch Benutzer von Lernmanagement-Systemen dies begrüßen würden, gibt es keine Realisierung dieser Funktion in den betrachteten Lernplattformen.

Eine Unterstützung der Lernenden wird durch die Funktionen 3, 4 und 5 bereitgestellt. Dabei traf die Tutorenbenachrichtigung nach schlechten Testergebnissen bei nur 31% der Umfrageteilnehmer auf Zustimmung und die Vereinfachung des Anmeldeprozesses sogar nur bei 29% der Umfrageteilnehmer. Wohingegen über 50% der Befragten die Anpassung der Lerninhalte an den Benutzer positiv einschätzten.
Aus den konkreten Datenschutzergebnissen lässt sich entnehmen, dass Tutoren in den meisten Lernmanagement-Systemen berechtigt sind, Testergebnisse einzusehen. Eine Ausnahme bietet bei OPAL mit den angebotenen Selbsttests, die nur für den Lernenden als Orientierung gedacht sind und nicht durch den Tutor eingesehen werden können. Auch wurde aufgezeigt, dass einige Lernmanagement-Systeme die Möglichkeit bieten, den Tutor nach Beendigung eines Tests zu benachrichtigen, unabhängig was für Testergebnisse angegeben wurden. Außerdem wird der Lernende beim Absenden darauf hingewiesen. Eine Tutorenbenachrichtigung nach schlechten Testergebnissen konnte in der Untersuchung nicht festgestellt werden.
Eine Vereinfachung des Anmeldeprozesses durch Technologien, die beispielsweise das „Single Sign-On" unterstützen, wird in den untersuchten Lernmanagement-Systemen in der Form angeboten, dass meist der Login-Zugang an einer Hochschule ausreicht, um auch Zugriff auf die von dieser Hochschule bereitgestellte Lernplattform zu erhalten. Bei OPAL wird dies beispielsweise durch die *Shibboleth-Technologie* realisiert. Dadurch benötigt der Benutzer nur noch die Kenntnis eines Passwortes, um sich zu authentifizieren.
Das Adaptieren von Lerninhalten, das von der Hälfte der Umfrageteilnehmer befürwortet wurde, kann einerseits durch Lernwegssteuerung und verschiedene Lernwege realisiert werden. Andererseits kann dies manuell durch den Lehrenden geschehen, indem er anhand von Profilangaben, Testergebnissen und dem Mitverfolgen von Lerneraktivitäten Rückschlüsse über benötigte Anpassungen zieht. Insbesondere die Einsicht in die Aktivitäten des Lernenden kann dabei ein sehr umfassendes Verhaltensbild preisgeben. Es sollte jedoch berücksichtigt werden, dass der einzelne Lernende eine solche Einsichtnahme eventuell nicht wünscht. Daher bieten Lernmanagement-Systeme wie OLAT die Möglichkeit an, Aktivitäten der Lernenden nur anonymisiert beziehungsweise pseudonymisiert zu betrachten. Auf diese Weise sind zwar Rückschlüsse auf die Verwendung einzelner Kurseinhalte möglich, aber die personenbezogene Beobachtung des Benutzerverhaltens ist nicht mehr gegeben. Jedoch ist somit auch keine Personalisierung anhand des Lernverhaltens möglich.

Die Funktionen 6. und 7., die den Benutzer eines eLearning-Systems dazu befähigen, den Zugriff auf seine personenbezogenen und sensiblen Daten zu regulieren und damit das Recht auf Informationelle Selbstbestimmung auszuüben, wurde von zwei Dritteln der Befragten befürwortet. Folgerichtig lehnten auch über 95% der Umfrageteilnehmer eine Datenverarbei-

tung in eLearning-Sytemen ab, in der jeder berechtigt ist, sensible und personenbezogene Daten von jedem anderen Benutzer einzusehen.
In der durchgeführten Datenschutzuntersuchung wurden auch Kriterien zur Umsetzung der Informationellen Selbstbestimmung betrachtet. Dabei wurde geprüft, ob Benutzern und insbesondere Lernenden Funktionalitäten zur Verfügung stehen, die es ermöglichen, die Datenerhebung, die Freigabe von personenbezogenen Daten und Aktivitätsdaten an ausgewählte Benutzergruppen und den Zweck der Verarbeitung zu konfigurieren. Außerdem sollte herausgearbeitet werden, inwieweit es für den Benutzer transparent ist, welche anderen Benutzer auf die eigenen personenbezogenen Daten zugegriffen haben.
Bei der Festlegung, welche personenbezogenen Daten von einem Teilnehmer erhoben werden, hat ein Lernender nur ein geringes Mitspracherecht. Entweder sind personenbezogene Daten durch Abfrage von externen Datenbanken schon enthalten oder werden bei der Anmeldung gefordert, so dass eine Verwendung ohne Angabe dieser Informationen nicht möglich ist. Nur bei optionalen Informationen, die zusätzlich angegeben werden können, kann der Benutzer wählen, ob er diese über sich zur Verfügung stellen möchte oder nicht.
Der Zweck der Datenverarbeitung seiner personenbezogenen Daten und Aktivitätsdaten kann durch den Lernenden selten beeinflusst werden. Insbesondere Aktivitätsdaten werden beispielsweise verwendet, um die Anwesenheit der Benutzer darzustellen oder das Lernverhalten aufzuzeichnen. Dabei kann nur der Lehrende oder der Administrator Einstellungen diesbezüglich vornehmen. So wurde in der untersuchten Installation von WebCT ermittelt, dass der Lehrende den Lernfortschritt eines Lernenden aufzeichnen kann und auch darüber entscheidet, ob der Lernende diesen einsehen darf. Bei OLAT können die Lernaktivitäten entweder anonym oder personalisiert aufgezeichnet werden. Auch dies wird vom Lehrenden festgelegt. ILIAS bietet eine Awareness-Funktion, bei der jeder Benutzer einstellen kann, ob er diese Funktion verwenden möchte, und ob er alle Benutzer der Lernplattform, die online sind, sehen möchte, oder nur diejenigen, die in den Gruppen und Kursen eingetragen sind, an denen er selbst teilnimmt. Wenn er sich dafür entscheidet, diese Funktion nicht zu nutzen, hat das keine Auswirkungen auf seine eigene Online-Anzeige für andere Benutzer, die diese Funktion aktiviert haben. Nur der Administrator ist in diesem Fall befähigt, die Awareness-Funktion vollständig zu deaktivieren.
Seine eigenen personenbezogenen Informationen anderen Benutzern zugänglich zu machen, wird von einigen Lernmanagement-Systemen angeboten. Allerdings ist die Preisgabe der personenbezogenen Daten nicht benutzer- oder gruppenbezogen möglich, sondern nur für alle Benutzer der Lernplattform oder keinen. Also eine differenzierte Freigabe für einzelne Benutzer oder spezielle Gruppen ist meist nicht möglich. So bieten Blackboard, OLAT und ILIAS die Funktionalität an, das eigene Benutzerprofil öffentlich zu machen. Bei ILIAS ist darüber hinaus realisiert, dass einzelne Informationen aus dem Profil ausgewählt werden können und nur diese den anderen Benutzern preisgegeben werden. Eine Veröffentlichung der personenbezogenen Daten kann bei den genannten Systemen wieder rückgängig gemacht werden, so dass der Benutzer auch nach der Preisgabe den Zugriff auf die Daten in seinem Benutzerprofil regulieren kann. ILIAS bietet als weitere Funktion an, Visitenkarten anderer Benutzer mit veröffentlichten Angaben zu speichern und extern zu verwalten. Dies bedeutet aber auch, dass diese Daten sich dem Einflussbereich des Eigentümers entziehen.

Eine Auskunft darüber zu erhalten, welche anderen Benutzer die eigenen, personenbezogenen Informationen eingesehen haben, wird durch die untersuchten Lernmanagement-Systeme nicht realisiert. Dies bedeutet, dass die stark befürwortete Möglichkeit, in eLearning-Systemen einzusehen, was andere über einen wissen, bisher offenbar nicht ausreichend unterstützt wird. Allgemein sind Funktionalitäten, die das Recht auf Informationelle Selbstbestimmung unterstützen können, nur geringfügig in den untersuchten Systemen enthalten. Wenn sie

vorhanden sind, werden diese Funktionen nur Lehrenden und Administratoren angeboten. Jedoch nicht denjenigen, die direkt betroffen sind.

7. Zusammenfassung und Ausblick

In der Diplomarbeit wurde eine intensive Betrachtung mit den ausgewählten Lernmanagement-Systemen bezüglich des Datenschutzes vorgenommen. So wurden Betreiber und Administratoren angeschrieben und um das Ausfüllen des selbst erstellten Fragebogens gebeten. Auch wurden weitere Quellen recherchiert, die das jeweilige System ebenfalls untersuchten. Schließlich wurden noch anhand eines Praxistests eigene Untersuchungen vorgenommen. Die so erhaltenen Informationen decken ein breites Feld ab, sind aber aufgrund der verschiedenartigen Quellen teilweise inhomogen. Dies mag einerseits daran liegen, dass unterschiedliche Versionen einer Lernplattform verwendet wurden oder aber auch an nicht korrekten Angaben der befragten Umfrageteilnehmer. Man sollte kritisch anmerken, dass es zur besseren Validierung der erhaltenen Informationen notwendig gewesen wäre, mehr Teilnehmer für die Befragung zu rekrutieren. Jedoch gestaltete es sich bereits als schwierig Ansprechpartner zu finden, die bereit waren, den Fragebogen auszufüllen. Dies mag daran liegen, dass die Betreiber und Administratoren einerseits wenig Zeit für derartige Umfragen haben, es jedoch auch andererseits sein kann, dass durch die ungenaue Gesetzeslage und damit verbundene Unsicherheiten von dem Ausfüllen des Fragebogens abgesehen wurde.

Betrachtet man die untersuchten Lernmanagement-Systeme nochmals zusammenfassend, lässt sich erkennen, dass bereits einige wichtige Mechanismen für den Datenschutz und der informationellen Selbstbestimmung integriert wurden oder zumindest derzeit eine Umsetzung geplant ist. Die bisherigen Ansätze sind jedoch noch nicht weitreichend und konsequent genug umgesetzt. Auch ist das erhaltene Gesamtbild, welches sich nach der durchgeführten Untersuchung ergibt, in Hinsicht auf die Aspekte des Datenschutzes und der Informationellen Selbstbestimmung noch viel zu inhomogen. Während einige Lernplattformen sich schon intensiv mit dem Aspekt des Datenschutzes auseinandersetzen, wird er in anderen Lernplattformen noch kaum beachtet. Vielfach fehlen Konfigurationsmöglichkeiten, um die Lernplattform den Datenschutzbedürfnissen der jeweiligen Benutzergruppe oder Institution anzupassen. Folglich werden Daten, die eigentlich im konkreten Fall nicht benötigt werden, dennoch erhoben, da dies die Lernplattform so vorsieht. In dieser Hinsicht sind insbesondere die Entwickler von Lernmanagement-Systemen gefragt, ihre Software dahingehend zu erweitern, dass eine gute Anpassung an die jeweiligen Datenschutzbestimmungen und -Bedürfnisse möglich ist. Auch sollten Institutionen darauf sensibilisiert werden, nicht nur auf die lehr- und lernrelevanten Funktionalitäten eines Lernmanagement-Systems zu achten. Vielmehr sollten in den Auswahlprozess auch Fragestellungen einfließen, die klären, ob das entsprechende System die benötigten Datenschutzaspekte umsetzt. Ein weiterer wichtiger Punkt ist die Schulung und Sensibilisierung von Administratoren zum Thema Datenschutz. Oftmals scheinen sich Administratoren aufgrund der komplexen Rechtslage unsicher zu sein, welche Maßnahmen bezüglich des Datenschutzes einzuhalten sind beziehungsweise welche Daten in welcher Form aufgezeichnet werden sollten. Hier ist es notwendig, zukünftig mehr Unterstützung anzubieten, da oft individuell zu entscheiden ist, wie mit bestimmten Informationen zu verfahren ist.

Die durchgeführte Untersuchung zeigt, dass der Lernende als zentraler Benutzer der Software vielfach für noch nicht mündig genug erklärt wird, um über seine personenbezogenen Daten selbst zu entscheiden. So obliegt es gewöhnlich einem Administrator oder Kursleiter zu entscheiden, wie mit personenbezogenen Daten des Lernenden zu verfahren ist. Es sollte jedoch vielmehr angestrebt werden, dem Lernenden mehr Kompetenzen in diesem Bereich zuzusprechen. Dies sollte besonders dann geschehen, wenn davon auszugehen ist, dass die Benutzer des Systems in der Lage sind, derartige Fragestellungen selbstständig zu beantworten. Ande-

renfalls kann auch durch zusätzliche Schulung und Sensibilisierung der Benutzer eine entsprechende Kompetenz aufgebaut werden.

In der vorliegenden Arbeit wurden die Ergebnisse der Untersuchung zu Lernmanagement-Systemen mit den Umfrageresultaten aus [Sta06] verglichen. Dieser Vergleich ergab, dass die bisher eingesetzten Mechanismen zur Gewährleistung des Datenschutzes und zur Förderung der Informationellen Selbstbestimmung noch nicht ausreichen, um die von den Benutzern geforderte Datenschutzfreundlichkeit zu erreichen. So sollten Lernende sich beispielsweise darüber informieren können, ob ihre personenbezogenen Daten von anderen eingesehen wurden.

Abbildungsverzeichnis

Abbildung 2.1:	Idealtypische Architektur eines Lernmanagement-Systems aus [Sch05] ……..	11
Abbildung 2.2:	Dreischichtige Architektur aus [Cha03] ……	16
Abbildung 2.3:	Das sicherheits- und datenschutzrelevante Umfeld eines Lernmanagement-Systems…….	17
Abbildung 2.4:	Gefahren für den Datenschutz und die Datensicherheit, die bei der Übermittlung von Daten über das Internet auftreten können (aus [Wei05]).	18
Abbildung 3.1:	Konfliktbereich Datenschutz-Hochschule; aus [Los06]……	28
Abbildung 6.1:	Konfiguration um persönliche Informationen öffentlich in Blackboard zugänglich zu machen…….	56
Abbildung 6.2:	Bearbeitung persönlicher Informationen eines Lernenden durch den Kursleiter in WebCT……...	61
Abbildung 6.3:	Historie der Inhaltsseiten, die ein Lernender in einem Kurs betrachtet hat (WebCT)……..	61
Abbildung 6.4:	Anzeige des persönlichen Profils eines ILIAS-Benutzers…….	64
Abbildung 6.5:	Anzeige des Lernfortschritts in ILIAS aus Sicht des Lernenden...	65
Abbildung 6.6:	Rechtevergabe durch den Administrator in Moodle……..	67
Abbildung 6.7:	Anzeige der Beutzeraktivitäten in Moodle…….....	67
Abbildung 6.8:	Konfiguration der Log-Files in OLAT……...	71
Abbildung 6.9:	Dialog aus BluES'n, der anfragt ob personenbezogene Daten übermittelt werden sollen……...	75
Abbildung 6.10:	Prozentualer Anteil der Befragten, die den Funktionen 1. bis 8. sehr oder etwas zu stimmten……..	81

Tabellenverzeichnis

Tabelle 2.1:	Vergleich von Lernmanagement-Systemen (Teil 1)……	14
Tabelle 2.2:	Vergleich von Lernmanagement-Systemen (Teil 2)……	15
Tabelle 3.1:	Übersicht über die Gewährleistung von Datenschutzanforderungen in verschiedenen Gesetzgebungen der Welt (aus [ISTPA])…….	27
Tabelle 5.1:	Übersicht über die Bewertungskriterien……...	50

Literatur und Quellenverzeichnis

[Bau02] Peter Baumgartner, Hartmut Häfele, Kornelia Maier-Häfele, 2002, E-Learning Praxishandbuch. Auswahl von Lernplattformen: Marktübersicht – Funktionen - Fachbegriffe. Innsbruck-Wien: StudienVerlag.

[BDSG] Bundesdatenschutzgesetz URL: https://www.datenschutzzentrum.de/material/recht/bdsg.htm (Stand: 09.09.2007)

[CAU97] CAUSE Task Force, 1997**,** Privacy and the Handling of Student Information in the Electronic Networked Environments of Colleges and Universities

[Cha03] Yuen-Yan Chan, Chi-Hong Leung und Joseph K. Liu, 2003, Evaluation on Security and Privacy of Web-Based Learning Systems, In: Proceedings of the "The 3rd IEEE International Conference on Advanced Learning Technologies"

[CLI] CLIX 5.0 Benutzeranleitung - Studenten -

[CLI01] Plattformbewertung: imc - CLIX® Campus 3.0, 2001

[CLI05] Sabine Allweier, 2005, CLIX 5.0 Benutzerhandbuch für Courseadministratoren

[CLI07] Anleitung für Studierende - CLIX Campus 6.1 , 2007, Karin Binder

[EUR02] Europäische Datenschutzrichtlinie für elektronische Kommunikation vom 12.07.2002, URL: http://www.datenschutz-berlin.de/recht/eu/rv/tk_med/tkdsr_de.htm (Stand: 09.09.2007)

[EUR06] Europäische Union, 2006, RICHTLINIE 2006/24/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG

[EUR95] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, URL: http://www.datenschutz-berlin.de/infomat/heft24/dde.htm (Stand: 09.09.2007)

[EMRK] Konvention zum Schutze der Menschenrechte und Grundfreiheiten (1950) URL: http://www.staatsvertraege.de/emrk.htm (Stand: 08.09.2007)

[Gla06] Christian Glameyer, 2006, Datenschutzrechtliche Fragen zum Einsatz von moodle an der FernUniversität in Hagen.

[Hae05] Hartmut Häfele, 2005, Top 16 Learning Management Systeme, http://virtual-learning.qualifizierung.com/top16.php

[Hal07] Brandon Hall 2007, URL: http://www.brandon-hall.com/free_resources/glossary.shtml) (Stand: 4.6.2007)

[Hes05] Michael Ronellenfitsch, Manfred Weitz, 2005, „Datenschutz in Schulen - Überblick und Materialien zur Durchführung des Datenschutzes an Schulen“

[Het03] Alexander Hettrich, Natascha Koroleva, 2003, “Marktstudie Learning Management Systeme (LMS) und Learning Content Management Systeme (LCMS)“, Stuttgart: Fraunhofer IRB Verlag

[ILIa] Hinweise zum Datenschutz, URL: https://ilias3.uni-stuttgart.de/ilias.php?baseClass=ilLMPresentationGUI&ref_id=13851 (Stand: 17.08.2007)

[ILIb] Benutzerdokumentation für ILIAS 3.8, URL: http://www.ilias.de/docu/goto_docu_cat_957.html

[ISTPA] International Security, Trust and Privacy Alliance (ISTPA), 2007, “Analysis of Privacy Principles: Making Privacy Operational”

[Klo06] Tomaž Klobučar, 2006, “Privacy and data protection in technology-enhanced professional learning”; In: Advanced International Conference on Telecommunications and International Conference on Internet and Web Applications and Services

[Kon81] Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (1981) URL: http://conventions.coe.int/Treaty/GER/Treaties/Html/108.htm (Stand: 08.09.2007)

[Lav96] N. Lavranos, 1996, „Datenschutz in Europa. Am Beispiel der Datenschutzrichtlinie, des Schengen Information Systems (SIS) und Europol, In: Datenschutz und Datensicherheit“, Juli 1996, pp. 400-408

[Los06] Kai-Uwe Loser, 2006, „Datenschutzprobleme in Blackboard: eLearning und informationelle Selbstbestimmung“

[MDLa] http://moodle.org/mod/forum/view.php?id=2662

[Mer] Marcus Merkel, „Usability-Evaluation der Virtuellen Fachbibliothek Ethnologie – E-VIFA“

[OECD] OECD, 2003, „Kurzfassung OECD-Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten„

[PAPI00] IEEE P1484.2/D7, 2000, “Draft Standard for Learning Technology — Public and Private Information (PAPI) for Learners (PAPI Learner)”

[Pau02] Morten Flate Paulsen, 2002, “European Experiences with Learning Management Systems”

[PRI] https://www.prime-project.eu/

[PRI06] Ronald Leenes, Simone Fischer-Hübner, 2006, Framework V2

[PRI07] Marco Casassa-Mont, Stefano Crosta, Thomas Kriegelstein, Dieter Sommer, 2007, „Architecture V2“

[Roß01a] Alexander Roßnagel, Andreas Pfitzmann, Hansjürgen Garstka, 2001, „Modernisierung des Datenschutzrechts - Gutachten im Auftrag des Bundesministeriums des Innern“

[Roß01b] Alexander Roßnagel, Andreas Pfitzmann, Hansjürgen Garstka, 2001, „Gutachtendesign – Modernisierung des Datenschutzrechts“

[Sch04] Viola Schmid, 2004, „CAST Workshop: Recht und IT-Sicherheit“

[Sch05] Rolf Schulmeister, 2005, „Lernplattformen für das virtuelle Lernen. Evaluation und Didaktik“, R. Oldenbourg Verlag: München

[Sha06] Peter Schaar, 2006, Peter Schaar fordert einheitlichen Datenschutzstandard für die polizeiliche Zusammenarbeit in Europa, URL: http://www.bfdi.bund.de/nn_531026/DE/Oeffentlichkeitsarbeit/RedenUndInterviews/2006/PeterSchaarFordertEinheitlichenDatenschutzstandardFuerDiePolizeilicheZusammenarbeitInEuropa.html (Stand: 08.09.2007)

[Sta06] Anne-Katrin Stange, 2006, „Konzeption und Realisierung einer Studie zu Einstellungen in Bezug auf Privacy-Aspekte im Bereich eLearning“

[ULD05] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, 2005, „Anforderungskatalog v 1.2 für die Begutachtung von IT-Produkten im Rahmen des Gütesiegelverfahrens beim ULD SH“

[ULD06] Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein, 2006, „Scoringsysteme zur Beurteilung der Kreditwürdigkeit - Chancen und Risiken für Verbraucher“

[ULD07] EuroPriSe - Kirsten Bock, 2007, “Spring Conference of European Data Protection Authorities”

[ULDFAQ] Häufig gestellte Fragen zum Datenschutz-Gütesiegel des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, URL: https://www.datenschutzzentrum.de/faq/guetesiegel.htm#12 (Stand: 11.09.2007)

[VZU] Urteil des Ersten Senats vom 15. Dezember 1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983 - 1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren über die Verfassungsbeschwerden, URL: http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm (Stand: 09.09.2007)

[WCTa] Privacy in the WebCT Environment URL: http://ils.unc.edu/daniel/210user/privacy.html (Stand: 03.08.2007)

[Wei05] Edgar R. Weippl, 2005, “Security in E-Learning”, Series: Advances in Information Security, Vol. 16

[Wil06] Fridolin Wild, 2006, “Institute of Information Systems and New Media, WUW”

[Wyl04] Richard Wyles, 2004, “Shortlisting of Learning Management System software –

Part I of LMS Evaluation”

[Yee06] G. Yee, Y. Xu, L. Korba, K. El-Khatib, 2006, “Privacy and Security in E-Learning”, In: The Future Directions in Distance Learning and Communication Technologies

Anhang A

Übersicht über für diese Arbeit relevante Inhalte des *Anforderungskatalog v1.2 für die Begutachtung von IT-Produkten im Rahmen des Gütesiegelverfahrens beim ULD SH* [ULD05]:

Komplex 1: Grundsätzliche technische Ausgestaltung von IT-Produkten

- Datensparsamkeit:
  - Ist es möglich, dass die Betroffenen pseudonym beziehungsweise anonym agieren?
  - Ist ein vollständiger Verzicht auf personenbezogene Daten möglich?
  - Welche personenbezogenen Daten sind wirklich erforderlich?
  - Wird auf das Anlegen von temporären Datenbeständen, wie beispielsweise unnötige Protokollierung, verzichtet beziehungsweise sind diese Daten vor unbefugten Zugriff gesichert?
  - Filtert der Empfänger Informationen, die übermittelt wurden, aber nicht zur Aufgabenerfüllung benötigt werden, heraus?
- Frühzeitiges Löschen, Anonymisieren oder Pseudonymisieren, wenn Daten noch erforderlich, aber Personenbezug verzichtbar:
  - Wie werden Löschen, Anonymisieren und Pseudonymisieren umgesetzt (automatisch / in welchen Abhängigkeiten)?
  - Wird zum fühest möglichen Zeitpunkt das Löschen, Anonymisieren oder Pseudonymisieren vorgenommen?
  - Sind die Pseudonyme so gewählt, dass sie nur mit größerem Aufwand depseudonymisiert werden können?
- Transparenz und Produktbeschreibung:
  - Ist die Transparenz der Datenverarbeitung (Datenflüsse, Speicherorte, Übermittlungswege, Zugriffsmöglichkeiten) gegenüber
    - Anwendern (Systemadministratoren und Benutzer) sowie
    - Betroffenen gewährleistet?
  - Ist die Produktbeschreibung
    - Verständlich?
    - Aktuell?
    - ermöglicht sie einen leichten Zugriff und eine geeignete Auswertung?
    - Wird das zu Grunde liegende Konzept ausreichend erläutert?
  - Besteht die Möglichkeit Einsicht in den Quelltext beziehungsweise das Gerät zu nehmen?

Komplex 2: Zulässigkeit der Datenverarbeitung

- Ermächtigungsgrundlage für die Verarbeitung von personenbezogenen Daten:
  - Gesetzliche Ermächtigung zur Verarbeitung von Daten,
    - Gibt es einen abgeschlossenen Katalog von Daten, die verarbeitet werden sollen?
    - Wenn nein: Beschränken sich die personenbezogenen Daten auf das Erforderliche?
    - Inwieweit sind Pseudonymisierungs- beziehungsweise Anonymisierungsgebote zu beachten?
  - Einwilligung des Betroffenen,
    - Stellt das Produkt eine Mustereinwilligungserklärung oder Hinweise zur Gestaltung der Einwilligungserklärung zur Verfügung (verarbeitende Stelle, Datenkategorien, die verarbeitet werden, geplante Übermittlungen und den Empfänger dieser Übermittlungen, Zweck der

Datenverarbeitung, Hinweis auf Freiwilligkeit und Widerrufbarkeit der Einwilligung)?
        - Gibt es eine Unterstützung des Einwilligungsprozesses durch das IT-System (dabei ist zu Beachten, dass in der Regel die Einwilligung vor der ersten Speicherung vorliegen muss)?
    - Besonderheiten der einzelnen Phasen der Datenverarbeitung:
        - Datenerhebung,
            - Wird die Herkunft personenbezogenen Daten dokumentiert?
            - Erfolgt eine Unterrichtung beziehungsweise Aufklärung des Betroffenen?
            - Erfolgt eine verdeckte Erhebung ohne Kenntnis des Betroffenen?
        - Übermittlung,
            - Erfolgt eine Protokollierung der Übermittlung?
            - Wird die Partei, die die Informationen erhält, darauf hingewiesen beziehungsweise dazu verpflichtet die Zweckbindung der erhaltenen Daten einzuhalten?
            - Kann diese Zweckbindung technisch überwacht werden?
        - Löschung nach Wegfall der Erfordernis,
            - Sind Fristen zur Löschung zu beachten?

- Einhaltung allgemeiner, datenschutzrechtlicher Grundsätze und Pflichten:
    - Zweckbindung,
        - Wie wird der Zweck dokumentiert, für den die personenbezogenen Daten erhoben werden?
        - Wird die Zweckbindung dadurch garantiert, dass personenbezogene Daten vermieden werden oder ihre Verkettbarkeit und damit eine zweckändernde Nutzung erschwert oder verhindert wird?
        - Gibt es eine Kennzeichnung von Datensätzen mit entsprechenden Zwecken sowie Zugriffsrechte, die andere Auswertungsmethoden oder eine Übermittlung einschränken?
    - Erleichterung der Umsetzung des Trennungsgebotes,
        - Gibt es Verfahren zur automatischen Pseudonymisierung beziehungsweise Anonymisierung?

Komplex 3: Technisch-organisatorische Maßnahmen: Begleitmaßnahmen zum Schutz der Betroffenen

- Maßnahmen, um unbefugten den Zugang zu Datenträgern zu verwehren,
- Maßnahmen, um zu verhindern, dass Daten unbefugt verarbeitet werden oder Unbefugten zur Kenntnis gelangen können:
    - Sind Methoden zur Authentisierung realisiert (sichere Passwörter, Sperrung bei Fehlversuchen)?
    - Können und werden ausreichend detaillierte Zugriffsrechte vergeben (Rollenkonzepte insbesondere Systemadministrator, Kontrollrollen)?
    - Wird die Vergabe dieser Rechte dokumentiert (Protokolldatei, externe Tools)?
    - Werden Systemadministrationsebene und Anwendungsebene ausreichend getrennt?
    - Werden Firewalls und Intrusion Detection& Respone Systems wirkungsvoll gegen unbefugte Eingriffe eingesetzt?

    - Sind die verwendeten Verschlüsselungsverfahren adäquat umgesetzt?
    - Sind Maßnahmen zum Löschen/Sperren/Zerstören der Daten bzw. Geräte bei unbefugten Eingriffen vorgesehen?
    - Gibt es Mechanismen, um die beabsichtigte und unbeabsichtigte jedoch unbefugte Weitergabe oder Offenbarung von Daten zu verhindern oder zu erschweren?
    - Wurden Maßnahmen ergriffen, um die Sensibilität der Verarbeiter zu steigern (z.B. durch automatisierte Warnhinweise)?
- Protokollierung von Datenverarbeitungsvorgängen,
    - Welche Daten werden ausschließlich automatisiert gespeichert?
    - Wie lassen sich die Protokolldaten auswerten? Gibt es automatisierte Auswertungsroutinen? Nach Welchen Kriterien? Welche Zugriffsrechte gibt es?
    - Wurden datenschutzrechtliche Anforderungen für die Verarbeitung der Protokolldaten geprüft?
    - Wann werden Protokolldaten gelöscht?
    - Sind gesetzliche Speicherfristen für die Protokolldatenbestände zu beachten?
- Weitere technische und organisatorische Maßnahmen,
    - Kommen Maßnahmen zur Sicherung der Integrität von Daten und Programmen zur Anwendung (zum Beispiel Virenschutz, Prüfsummen, digitale Signaturen, Deaktivieren von möglicherweise schädigenden Funktionen)?
    - Werden ausreichende Maßnahmen zur Sicherung der Verfügbarkeit ergriffen (Beispielsweise durch Sicherheitskopien, Zugangs-, Zutritts- und Zugriffsrechte auch für Stellvertreter)?
    - Wird die Vertraulichkeit von Datenbeständen bei Speicherung und Übermittlung ausreichend sichergestellt?
- Geeignete Unterstützung von Tests und Evaluationen durch das Programm für eine Datenschutzkontrolle,
- Pflichten nach der Datenschutzverordnung,
    - Wird die Erstellung des Sicherheitskonzeptes und der Risikoanalyse unterstützt?

Komplex 4: Rechte der Betroffenen

- Aufklärung und Benachrichtigung:
    - Inwieweit wird Aufklärung und Benachrichtigung vom IT-Produkt geleistet oder unterstützt?
    - Gibt es besondere Maßnahmen, um die Transparenz der Datenverarbeitung für den Betroffenen sicherzustellen?
- Auskunft:
    - Gibt es eine automatisierte Auskunftsbearbeitung durch das IT-Produnkt?
    - Erfasst die Auskunftsmöglichkeit den gesamten Auskunftsanspruch (gespeicherte Daten, Zweck und Rechtsgrundlage, Herkunft und Empfängerkreis, Funktionsweise) von automatisierten Verfahren?
- Benachrichtigung, Löschung, Sperrung, Einwand beziehungsweise Widerspruch:
    - Gibt es automatisierte Berichtigungsbearbeitung vom IT-Produkt?
    - Wird vollständig und irreversibel gelöscht?
    - Gibt es eine Möglichkeit, die Datensätze so zu kennzeichnen, dass sie für die normale Bearbeitung nicht zur Verfügung stehen, aber gleichwohl gespeichert bleiben?
    - Gibt es eine Technische Unterstützung des Widerspruchrechtes?

Anhang B

Unterstützung des Datenschutzes in Lernmanagement-Systemen

Allgemeine Angaben zum Lernmanagement-System (LMS)

Name des LMS:
Version des LMS:
Wie viele Benutzer sind in dem LMS angemeldet?

Der Fragebogen ist in zwölf Fragekomplexe gegliedert. Die meisten Fragen sind als ja/nein Antworten formuliert. Alle weiteren Fragen sind als Freitextantworten angelegt und sind dafür gedacht, dass die jeweiligen Charakteristika des LMS näher erläutert werden. Sollten Sie noch Fragen haben, so können Sie mich unter as024121@mail.inf.tu-dresden.de erreichen.

Bitte beziehen Sie sich bei der Beantwortung der weiteren Fragen auf die oben angegebene Version des LMS!

Als personenbezogene Daten sind für die Beantwortung des Fragebogens Informationen anzusehen, die durch den Benutzer selbst angegeben werden oder durch die Interaktion mit dem LMS erhoben werden. Zu personenbezogenen Daten gehören beispielsweise Benutzerprofile, die identifizierende Informationen enthalten können, Lehr- und Lernaktivitäten, Bewertungen, Noten und übermittelte Verkehrsdaten, die Informationen über den lokalen Standort enthalten.

1. Fragekomplex

Hat der Benutzer die Möglichkeit die über ihn gespeicherten persönlichen Informationen direkt über die Lernplattform einzusehen?	☐Ja ☐Nein
Hat der Benutzer die Möglichkeit, seine vom LMS protokollierten Benutzeraktivitäten und Verbindungsdaten, direkt über die Lernplattform einzusehen?	☐Ja ☐Nein
Wenn eine direkte Einsicht nicht möglich ist, gibt es dann eine andere Möglichkeit für den Benutzer die über ihn gesammelten Daten einzusehen?	
Weitere Kommentare zu diesem Themenkomplex:	

2. Fragekomplex

Wird dem Benutzer durch das LMS die Möglichkeit zur Modifikation	☐Ja ☐Nein

seiner personenbezogenen Daten direkt angeboten?	
Wenn nein, gibt es eine andere Möglichkeit seine personenbezogenen Daten zu modifizieren?	
Wird dem Benutzer ermöglicht, auf die Verarbeitung seiner personenbezogenen Daten weitreichenden Einfluss zu nehmen? Indem er selbst festlegen kann welche persönlichen Daten und Aktivitätsdaten über ihn gespeichert werden sollen?	☐Ja ☐Nein
Indem er den Zweck konfigurieren kann, für den seine personenbezogenen Daten genutzt werden sollen?	☐Ja ☐Nein
Indem er den Zugriff auf seine personenbezogenen Daten so konfigurieren kann, dass diese nur bestimmten Benutzergruppen zugänglich gemacht werden?	☐Ja ☐Nein
Indem er einsehen kann, ob und wer bestimmte personenbezogene Daten über ihn abgerufen hat bzw. weiß?	☐Ja ☐Nein
Weitere Kommentare zu diesem Themenkomplex:	

3. Fragekomplex

Unterstützt das LMS, dass eine Einwilligung der Benutzer zur Datenerhebung und Verarbeitung eingeholt wird?	☐Ja ☐Nein
Wenn ja, in welcher Form wird die Einwilligung des Benutzers eingeholt?	
Kann der Benutzer die Einwilligung widerrufen?	☐Ja ☐Nein
Wird dabei mit besonderer Sorgfalt bei der Datenerhebung von Kindern und Jugendlichen vorgegangen?	☐Ja ☐Nein
Wenn ja, erläutern Sie dies bitte:	
Wird der Benutzer bei Änderungen der Konditionen der Verarbeitung informiert?	☐Ja ☐Nein
Weitere Kommentare zu diesem Themenkomplex:	

4. Fragekomplex

Wird der Benutzer darüber informiert,… …welche personenbezogenen Daten über ihn gesammelt werden?	☐Ja ☐Nein
…wer personenbezogene Daten über ihn sammelt?	☐Ja ☐Nein
…zu welchem Zweck diese Daten gesammelt werden?	☐Ja ☐Nein
…welche Sicherheitsvorkehrungen zum Schutz der Daten im Einsatz sind bzw. was nicht geschützt werden kann?	☐Ja ☐Nein
…welche anderen Benutzer des LMS Zugriff auf die	☐Ja ☐Nein

personenbezogenen Daten erhalten?	
…wenn eine Weitergabe seiner personenbezogenen Daten an Dritte erfolgt?	☐Ja ☐Nein
Unterstützt das LMS die Anfertigung bzw. Platzierung von Datenschutzerklärungen / Privacy Policies?	☐Ja ☐Nein
Besteht die Möglichkeit für die Benutzer des LMS zu überprüfen, ob die Zusicherungen (bspw. aus der Datenschutzerklärung) eingehalten werden?	☐Ja ☐Nein
Wenn ja, erläutern Sie dies bitte:	
Weitere Kommentare zu diesem Themenkomplex:	

5. Fragekomplex

Ist eine pseudonyme Nutzung der Lernplattform möglich bzw. können mehrere (Teil-)Identitäten pro Benutzer verwendet werden?	☐Ja ☐Nein
Wenn ja, in welchem Umfang ist die Lernplattform pseudonym nutzbar?	
Ist eine anonyme Nutzung der Lernplattform möglich?	☐Ja ☐Nein
Wenn ja, in welchem Umfang ist die Lernplattform anonym nutzbar?	
Sammelt die Lernplattform Ihrer Meinung nach mehr personenbezogene Daten als für den vorgesehenen Zweck erforderlich?	☐Ja ☐Nein
Wenn ja, auf welche personenbezogenen Daten könnte verzichtet werden?	
Verzichtet das LMS Ihrer Meinung nach auf die Speicherung bzw. Weiterverarbeitung von Informationen, die beim Datenaustausch übermittelt werden (Verkehrsdaten), aber nicht der Aufgabenerfüllung dienen?	☐Ja ☐Nein
Werden die Benutzer Ihrer Meinung nach durch die Lernplattform für den Schutz von personenbezogenen Daten sensibilisiert?	☐Ja ☐Nein:
Wenn ja, erläutern Sie dies bitte:	
Weitere Kommentare zu diesem Themenkomplex:	

6. Fragekomplex

Wird gewährleistet, dass die Daten, die über den Benutzer gesammelt werden sachlich richtig, vollständig, und aktuell sind?	☐Ja ☐Nein
Wenn ja, wie wird das gewährleistet?	
Weitere Kommentare zu diesem Themenkomplex:	

7. Fragekomplex

Ist der Zeck der Datensammlung vor der Erhebung festgelegt?	☐Ja ☐Nein
Wird durch das LMS gewährleistet, dass nur die Personen Zugriff auf personenbezogene Daten und Aktivitätsaufzeichnungen anderer Benutzer erhalten, die diese direkt benötigen?	☐Ja ☐Nein
Werden die Daten mit anderen Datenbanken verknüpft oder weiterverarbeitet?	☐Ja ☐Nein
Weitere Kommentare zu diesem Themenkomplex:	

8. Fragekomplex

Ist die Löschung von personenbezogenen und sensiblen Daten durch das LMS vorgesehen?	☐Ja ☐Nein
Wenn ja, bietet das LMS Löschfristen für sensible und personenbezogene Daten an, die für die Diensterbringung nicht mehr erforderlich sind?	☐Ja ☐Nein
Sieht die Lernplattform eine Archivierung von personenbezogenen Daten vor?	☐Ja ☐Nein
Werden personenbezogene Daten nach Beendigung der Erforderlichkeit anonymisiert, falls sie nicht gelöscht werden?	☐Ja ☐Nein
Wie wird mit aufgezeichneten Kommunikationsdaten, in die der Benutzer involviert war, bzw. Diskussionsbeiträge des Benutzers verfahren, wenn er das LMS nicht mehr nutzt?	
Weitere Kommentare zu diesem Themenkomplex:	

9. Fragekomplex

Unterstützt das LMS eine gesicherte Übertragung von sensiblen und persönlichen Daten, wie etwa Passwörter, Benutzerprofile, Noten und Bewertungen von Benutzern, über das Internet?	☐Ja ☐Nein
Wenn ja, welche Techniken werden dafür eingesetzt? Bitte geben Sie hier auch an, ob die Techniken direkt in der Lernplattform enthalten sind, als Erweiterung integriert werden können.	
Unterstützt das LMS eine gesicherte Übertragung bei jedem Datenaustausch von sensiblen und personenbezogenen Daten?	☐Ja ☐Nein
Wenn nein, wann wird eine gesicherte Übertragung von sensiblen und personenbezogenen Daten gewährleistet?	
Können autorisierte Personen die Schutzmaßnahmen für die Übertragung von persönlichen und sensiblen Daten global für alle Teilnehmer konfigurieren?	☐Ja ☐Nein

Hat jeder Benutzer der Lernplattform die Möglichkeit, die Schutzmaßnahmen für seinen Datentransfer mit dem LMS zu konfigurieren?	☐Ja ☐Nein
Welche Standardeinstellungen sind durch das LMS zur Übertragung von sensiblen und persönlichen Daten voreingestellt?	
Weitere Kommentare zu diesem Themenkomplex:	

10. Fragekomplex

Unterstützt das LMS eine geschützte Datenhaltung von sensiblen und persönlichen Daten?	☐Ja ☐Nein
Wenn ja, welche Techniken werden dafür eingesetzt? Bitte geben Sie hier auch an, ob die Techniken direkt in der Lernplattform enthalten sind, als Erweiterung integriert werden können.	
Unterstützt das LMS eine geschützte Datenhaltung von allen sensiblen und persönlichen Daten, die durch die Verwendung des LMS entstehen oder durch den Benutzer eingegeben werden?	☐Ja ☐Nein
Wenn nein, welche Daten werden geschützt gespeichert?	
Können durch autorisierte Personen die Schutzmaßnahmen für die Datenhaltung von sensiblen und persönlichen Daten global für alle Teilnehmer konfiguriert werden?	☐Ja ☐Nein
Hat jeder Benutzer der Lernplattform die Möglichkeit die Schutzmaßnahmen für die Datenhaltung seiner sensiblen und persönlichen Daten zu konfigurieren?	☐Ja ☐Nein
Welche Standardeinstellungen sind durch das LMS zur Datenhaltung von sensiblen und persönlichen Daten voreingestellt?	
Weitere Kommentare zu diesem Themenkomplex:	

11. Fragekomplex

Ist die Möglichkeit gegeben, den Benutzern des LMS eindeutige Identitäten zuzuweisen bzw. zu authentifizieren?	☐Ja ☐Nein
Wenn ja, welche Möglichkeiten und Techniken werden dafür eingesetzt? Bitte geben Sie hier auch an, ob die Techniken direkt in der Lernplattform enthalten sind oder als Erweiterung integriert werden können.	

Haben die Benutzer des LMS unterschiedliche Rollen, die sich durch unterschiedliche Rechte und Möglichkeiten darstellen?	☐Ja ☐Nein
Werden die unterschiedlichen Rechte und Möglichkeiten durch das LMS technisch sichergestellt?	☐Ja ☐Nein
Ist ersichtlich, welche Auswirkungen die verschiedenen Rechte auf die Privatsphäre der anderen Benutzer des LMS haben…	
…durch den Benutzer, der die Rechte anderen zuteilt?	☐Ja ☐Nein
…durch den Benutzer, der die Rechte besitzt?	☐Ja ☐Nein
…durch den Benutzer, der durch die Rechte Dritter in seiner Privatsphäre beeinträchtigt werden könnte?	☐Ja ☐Nein
Können ausschließlich autorisierte Personen der Lernplattform Rollen und Rechte an andere Benutzer vergeben?	☐Ja ☐Nein
Wenn nein, erläutern Sie dies bitte:	
Kann ein angemeldeter Benutzer mehrere unterschiedliche Rollen in einem Kurs des LMS einnehmen (bspw. Lehrender und Studierender)?	☐Ja ☐Nein
Weitere Kommentare zu diesem Themenkomplex:	

12. Fragekomplex

Werden sensible oder personenbezogene Daten gespeichert, wie bspw. die Aktivitäten eines Benutzers bzw. Zugriffe eines Benutzers auf Inhalte und Funktionen innerhalb des LMS, um den Sicherheitszustand des Systems zu protokollieren?	☐Ja ☐Nein
Wenn ja, welche Daten, die die Benutzer betreffen, werden dabei gesammelt, um den Sicherheitszustand des Systems zu überwachen?	
Können sicherheitsrelevante Ereignisse einem bestimmten Benutzer/Verursacher zugeordnet werden?	☐Ja ☐Nein
Sind personenbezogene Daten vor unbefugter Einsicht, Modifikation und Löschung geschützt?	☐Ja ☐Nein
Wenn ja, erläutern Sie bitte durch welche Maßnahmen.	
Werden durch das LMS folgende Standards unterstützt? IMS Learner Information Package (LIP)	☐Ja ☐Nein
IEEE Public and Private Information (PAPI)	☐Ja ☐Nein
Ist die Lernplattform angemessenen gegen externe Angreifer geschützt?	☐Ja ☐Nein
Werden sichere Login-Passwörter generiert bzw. die Erstellung solcher Passwörter durch das System unterstützt?	☐Ja ☐Nein

Weitere Kommentare zu diesem Themenkomplex:

Anhang C

	BluES'n (1)	BluES'n (2)	WebCT
Version	Prototype build.947	keine	4.1.5.8 Campus Edition (etwa 1000 Benutzer)
Unterstützung einer gesicherten Übertragung von sensiblen und persönlichen Daten über das Internet durch das LMS:	Ja, immer möglich; BluES'n integriert die Schnittstelle zum lokalen PRIME-Client; Verschlüsselung der Datenkommunikation (HTTPS geplant für APv2).	Ja, BluES verwendet dafür die Techniken, die ihm von der PRIME-Plattform angeboten werden. Eine geschützte Übertragung kann immer gewährleistet werden.	Ja, mittels SSL.
Konfigurationsmöglichkeiten:	Jeder Benutzer kann lokal im PRIME-Client Konfigurationen vornehmen.	Konfiguration außerhalb des LMS, da von PRIME gemanaged.	Administrator legt global fest, ob Passwörter abgesichert sind oder alles absichert ist oder die Funktion auf inaktiv gesetzt ist.
Standarteinstellungen:	Bisher das, was PRIME bietet.	K.A.	K.A.
Unterstützung einer geschützten Datenhaltung von sensiblen und persönlichen Daten:	Die Datenhaltung, egal ob auf Client oder Server Seite wird nicht verschlüsselt durch BluES oder PRIME in Datenbanken abgelegt. Der Zugang selbst ist durch ein Log-in/Passwort geschützt, aber die Daten sind nicht verschlüsselt. Für eine Verschlüsselung muss der Benutzer selbst sorgen (Bitlocker), Server speichert nur das, was er dringend benötigt unter Pseudonym, partieller Identität wie beispielsweise Kommunikationsdaten in Foren und Chats. Diese werden ungeschützt gespeichert.	Ja, durch PRIME-Techniken, alle sensiblen Daten sind geschützt.	Ja, durch organisatorische Vorkehrungen und Zugriffsrechte nur für autorisierte Rollen. Personenbezogene Daten werden ungeschützt in Klartext gespeichert. Weitere Maßnahmen nur durch externe Regelung möglich.
Konfiguration:	nein	Systemadministrator serverseitig, Benutzer clientseitig selbst verantwortlich	Gibt keine Konfiguration
Standarteinstellung:	Unverschlüsselt, Passwort gesetzt	K.A.	K.A.
Eindeutige Authentifizierung eines Benutzers:	Durch PRIME-Schnittstelle werden Credentials zur Autorisierung (ein Nutzer zertifiziert eine oder mehrere Eigenschaften) zur Verfügung gestellt. Eindeutige Pseudonyme, die durch den Benutzer	Ja, ist möglich.	Ja, ticket-basierte Authentifizierung oder WebCT-Authentifizierung über eine Domain.

	gewählt werden, dienen zur Identifizierung.		
Rollenmodell:	Es gibt nur den Owner eines Workspaces und dessen Teilnehmer	ja	ja
Rechte und deren technische Durchsetzung:	Der Owner eines Workspaces hat mehr Rechte als die anderen Teilnehmer.	K.A.	Ja, Rechte werden technisch sichergestellt.
Auskunft über Auswirkungen der Rechte auf die Privatheit der anderen Benutzer:	nein	nein	K.A.
Rollenerstellung und Vergabe:	Owner kann Rechte an andere Teilnehmer vergeben für den Workspace, wo er Owner ist.	Vergabe nur durch autorisierte Personen.	Festgelegte Rollen, eigene können nicht hinzugefügt werden; Vergabe der Rollen durch den Administrator
Geltungsbereich der Rechte:	Je Workspace	K.A.	Je Kurs
Mehrere Rollen durch einen Benutzer in einem Kurs einnehmbar:	Ja, ein Benutzer kann mehrere Rollen in der Lernplattform einnehmen.	Ja, aber das Rollenkonzept ist noch finalisiert.	Jeder Benutzer bzw. eine Benutzer-ID kann nur eine Rolle einnehmen
Protokollierung von Zugriffs- und Aktivitätsdaten zur Überwachung des Sicherheitszustandes:	Nein, aber serverseitig können theoretisch Logs aktiviert werden, so dass ersichtlich ist, welches Pseudonym wann was geöffnet, betreten verändert hat.	Nein, aber solche Daten werden gespeichert für Awarenessinformationen, damit die Kollaboration zwischen Benutzern unterstützt werden kann.	Zumindest auf WebCT-Ebene keine Aufzeichnungen für den Sicherheitszustand. IP wird nicht geloggt. Aber allgemein: Aktivitätsinformationen werden aufgezeichnet (erstes und letztes Login und welche Aktionen).
Sicherheitsrelevante Ereignisse einem Verursacher zuordnen:	Das Pseudonym des Benutzers, das versucht hat etwas zu öffnen/ändern ist ersichtlich. Je nach Wahl des Pseudonyms/Angabe von persönlichen Daten ist auch ein konkreter Benutzer ermittelbar.	ja	K.A.
Schutz vor unbefugter Einsicht, Löschung und Modifikation:	Ja, Änderungen auf dem Client sind durch Fremde nicht möglich, solange das OS korrekt eingestellt ist. Änderungen auf dem Server müssen per Credential oder eindeutigem Pseudonym belegt werden.	Ja, durch noch zu realisierende Access Control Policies.	Ja, durch das Rechtemanagement
Unterstützung der Spezifikation PAPI und IMS LIP:	nein/nein	K.A.	K.A.
Lernplattform angemessen gegen externe Angreifer geschützt:	nein	Ja, durch gesicherte Speicherung der Daten sowie Schutz der Kommunikation.	Ja
Sichere Login-Passwörter:	Es gibt in dem Sinne keine Passwörter. Dies wird per Credentials geregelt.	nein	Passwort wird beim ersten Login vom Benutzer geändert, Mindest- und Maximallänge lässt sich festlegen.
Direkte Einsicht von gespeicherten persönlichen Infor-	Ja, die Daten, die lokal bei ihm in BluES	Ist noch zu realisieren.	K.A.

mationen über die Lernplattform:	Client/PRIME Client abgelegt sind, sind einsehbar. Die Daten auf dem Server (im wesentlichen die Pseudonyme, geschriebene Mail-Forumsnachrichten und Chatnachrichten) können über den Client abgerufen werden.		
Direkte Einsicht von Benutzeraktivitäten und Verbindungsdaten, die vom LMS gespeichert werden:	K.A.	Ist noch zu realisieren	K.A.
Weitere Möglichkeiten:			
Möglichkeit zur direkten Modifikation von personenbezogenen Daten durch den Benutzer:	K.A.	ja	K.A.
Benutzer kann festlegen welche Daten über ihn gespeichert werden:	Nein, der Benutzer kann nur entscheiden, ob er die geforderten Daten freigeben möchte.	Ja, der Benutzer wird informiert, welche Daten von ihm verlangt werden und er kann entscheiden, ob er die Daten preisgibt. Allerdings kann die Diensterbringung davon abhängen, dass er die geforderten Daten liefert.	nein
Benutzer kann Zweck konfigurieren, für den seine Daten verwendet werden dürfen:	Ja, durch Data Handling Policies von PRIME kann er angeben, wie seine angegebenen Daten zu verwenden sind.	Ja, könnte realisiert werden, ist aber noch nicht umgesetzt.	nein
Benutzer kann entscheiden, welchen Benutzergruppen er seine Daten zugänglich macht:	Ja, durch Data Handling Policies von PRIME, Release Policies von PRIME und der Rechtekontrolle von BluES`n.	ja	nein
Benutzer kann einsehen, ob und wer welche persönlichen Daten über ihn abgerufen hat bzw. weiß:	Nein, was andere Benutzer über einen wissen kann er nicht einsehen. Abrufe von Daten durch den Server beim Client können allerdings im Datatrack nachvollzogen werden (welches Datum für was, wann).	Ja, bspw. bei Testergebnissen. Nein, bei Informationen, die er für eine Kontaktaufnahme bereitstellt, wie Interessen und Hobbys.	nein
Einwilligungserklärung des Benutzers für die Datenverarbeitung durch LMS zur Verfügung gestellt:	Ja, bei der Übermittlung von personenbezogenen Daten erscheint ein „Ask-send-Data Dialog“ von PRIME und fragt nach der Einwilligung.	Ja, beim Start der Anwendung wird eine Privacy Policy angezeigt, die den Benutzer allgemein informiert. Immer wenn Daten abgefragt werden, erhält der Benutzer eine Information (welche Daten und wofür). Er kann die Daten auswählen bzw. sich entscheiden nichts zu	Im untersuchten Fall wird die Datenschutzerklärung mit der Beantragung des Logins vor Verwendung des LMS unterschrieben und abgegeben.

		senden (Diensterbringung kann davon abhängen)	
Widerrufen der Einwilligung:	nein	Da immer vor der Datenübertragung gefragt wird, ist widerrufen nicht notwendig.	Ja, durch E-Mail an Verantwortlichen, aber nicht mittels WebCT.
Besondere Sorgfalt bei der Verarbeitung von persönlichen Daten von Kindern:	nein	nein	Bei Teilnehmern unter 18 Jahren müssen die Eltern der Datenverarbeitung zustimmen. Wird aber nicht in WebCT realisiert.
Informieren des Benutzers bei Veränderungen der Konditionen der Verarbeitung:	nein	K.A.	K.A.
Informieren des Benutzers über die Art der personenbezogenen Daten, die über ihn gesammelt werden sollen:	ja	ja	In der Datenschutzbelehrung wird darauf hingewiesen, welche personenbezogenen Daten gesammelt werden.
Informieren des Benutzers über den Verantwortlichen der Datenverarbeitung:	K.A.	ja	ja
Informieren des Benutzers über den Zweck der Datenverarbeitung:	ja	ja	ja
Informieren des Benutzers über die Sicherheitsvorkehrungen, die zum Schutz der Daten im Einsatz sind:	ja	nein	nein
Informieren des Benutzers, welche anderen Benutzer Zugriff auf seine Daten haben:	ja	ja	nein
Informieren des Benutzers, wenn eine Weitergabe seiner Daten an dritte erfolgt:	ja	nein	Nein, eine Weitergabe ist auch nicht vorgesehen.
Bereitstellung einer Datenschutzerklärung durch das LMS:	ja	ja	Nein, Datenschutzerklärung wird im untersuchten Fall außerhalb des LMS angeboten.
Angegebene Zusicherungen durch Benutzer nachprüfbar:	Ja, wäre theoretisch möglich.	K.A. schwierig, wie soll der Benutzer überprüfen, ob die Daten nicht weitergegeben wurden?	K.A.
Pseudonyme Nutzung der Lernplattform:	Ja, Benutzer kann entscheiden unter welchem Pseudonym er in welchem Workspace auftritt. Teilweise kann er sogar innerhalb eines Workspaces das Pseudonym wechseln (zwischen funktionalen Modulen). Er kann entscheiden, ob er Pseudonyme wieder verwenden will (wichtig für Chat, Mailforum und gemeinsame Materialerstellung).	Ja, für jede Aktion kann ein anderes Pseudonym verwendet werden. Allerdings sind Einschränkungen durch serverseitige Policies möglich (beispielsweise nur ein Pseudonym pro Workspace, damit ein Tutorden Lernfortschritt beobachten oder Hilfestellung geben kann).	nein

Anonyme Nutzung der Lernplattform:	Ja, mittels Tor und ähnlichen ist eine anonyme Datenkommunikation möglich. Auf Anwendungsebene kann ständig ein neues Pseudonym für jede Aktion verwendet werden, so dass keine Wiedererkennung möglich ist.	Ja, wenn es für Ressourcen keine Zugriffsregeln gibt, die die Preisgabe von persönlichen Daten verlangen (Access Control Policies). Es ist allerdings nicht möglich nur anonym zu arbeiten (Material soll dem Autor zuzuordnen sein oder Lernende sollen unterstützt werden können).	nein
Werden mehr sensible Informationen gesammelt als notwendig:	Erklärtes Ziel ist so wenig wie möglich zu sammeln.	nein	K.A.
Wird auf die Weiterverarbeitung von Verkehrsdaten verzichtet:	K.A.	ja	IP-Adresse wird nicht dargestellt.
Sensibilisiert die Lernplattform den Benutzer hinsichtlich Datenschutz:	K.A.	ja	K.A.
Wird gewährleistet, dass die Informationen, die über den Benutzer gesammelt werden, wenn benötigt sachlich richtig, vollständig und aktuell sind:	nein	Bei zertifizierten Daten wird dies gewährleistet, bei unzertifizierten nicht. Die meisten personenbezogenen Daten fallen zur Zeit an, wenn der Benutzer Kontaktinformationen (Profile) hinterlegt. Welche Informationen aber solche Profile enthalten, ist dem Benutzer freigestellt (außer einem Pseudonym, um überhaupt eine Zuordnung treffen zu können).	Ja, durch vorherige Anmeldung und Nachweis einer Mitgliedschaft in einer Bildungseinrichtung. Diese Daten werden in der Lernumgebung verwendet.
Kann Zweckbindung technisch durch das LMS überwacht werden?	Ja, durch Data Handling Policies.	K.A.	K.A.
Festlegung des Zweckes der Datenersammlung vor der Erhebung:	ja	ja	Ja, in der Datenschutzbelehrung
Wird gewährleistet, dass nur Personen Zugriff auf personenbezogene Daten erhalten, die sie auch benötigen:	ja	Wie wird festgestellt wer was direkt benötigt?	Ja, durch die Rollenzuweisungen dürfen Kursleiter Lernaktivitäten und Testergebnisse ihrer Lernenden einsehen
Verknüpfung von Datenbanken und Weiterverarbeitung der Daten:	nein	ja	nein
Ist die Löschung von personenbezogenen und sensiblen Daten durch das LMS vorgesehen:	ja	ja	Ja, nach 6 Wochen Inaktivität wird ein Benutzer gelöscht (persönliche Angaben, Aktivitätsdaten, alle Nachrichten in den Kursen), LMS dann nicht mehr nutzbar.
Löschfristen, wenn Erforderlichkeit wegfällt:	nein	Nein, ist noch zu realisieren.	K.A.
Archivierung von personen-	ja	ja	nein

bezogenen Daten:			
Anonymisieren von personenbezogenen Daten, wenn nicht gelöscht:	nein	Nein, sollte aber so gemacht werden.	K.A.
Handhabung von Kommunikationsdaten, wie Chataufzeichnungen oder Diskussionsbeiträge in Foren:	Diskussionsbeiträge im Mailforum und die Chathistory werden auf dem Server persistent gespeichert. Sie sind für alle berechtigten Benutzer des Workspaces einsehbar.	Benutzer können in BluES'n nicht direkt erkannt werden. Die verwendeten Pseudonyme sind der realen Identität nicht zuzuordnen. Es sollten nicht alle Pseudonyme gleichzeitig abgemeldet werden, da sie sonst verkettbar sind.	K.A.
Zusatz:	Datatrack: lokal auf dem Client werden Daten gesammelt (wem habe ich was in welchem Kontext gezeigt; sind nicht zur Protokollierung des Sicherheitszustandes gedacht)		

	Blackboard	OLAT	CLIX Campus
Version	7.2 (8700 Benutzer)	OPAL 2.1 (über 16000 Benutzer)	5 (ca. 22000 Benutzer)
Unterstützung einer gesicherten Übertragung von sensiblen und persönlichen Daten über das Internet durch das LMS:	Ja, mittels SSL ist eine gesicherte Übertragung immer möglich.	Ja, mittels SSL ist eine gesicherte Übertragung immer möglich.	Ja, das LMS wird in einer gesicherten Internetumgebung betrieben (https). Darüber hinaus obliegt die gesamte Technik den Sicherheitsbestimmungen des Rechenzentrums mit allen notwendigen Zugriffsbeschränkungen. Eine gesicherte Übertragung ist immer gewährleistet.
Konfigurationsmöglichkeiten:	Ja, durch autorisierte Personen.	Ja, durch autorisierte Personen.	Ja, durch autorisierte Personen.
Standarteinstellungen:	K.A.	SSL	K.A.
Unterstützung einer geschützten Datenhaltung von sensiblen und persönlichen Daten:	Ja, alle personenbezogenen Daten können geschützt werden.	Ja, alle personenbezogenen Daten können geschützt werden durch zentrale Datenhaltung auf dem Server – damit werden alle technischen und organisatorischen Mittel ausgeschöpft, entsprechend dem aktuellen Stand der Technik, die Daten zu und Server abzusichern und zu schützen.	Ja, aber eine gesicherte Datenhaltung kann nicht für alle personenbezogenen und sensiblen Daten unterstützt werden.
Konfiguration:	Ja, durch autorisierte Personen.	Ja, durch autorisierte Personen.	Ja, durch autorisierte Personen.
Standarteinstellung:	K.A.	K.A.	K.A.
Eindeutige Authentifizierung eines Benutzers:	ja	ja OPAL: Übernahme der Identitäten aus den Hochschulen via Shibboleth; OLAT: Eindeutige Identität durch derzeit übliche Registrierungsmechanismen	Ja, LDAP Authentifikation.
Rollenmodell:	ja	ja	ja
Rechte und deren technische Durchsetzung:	ja	ja	ja
Auskunft über Auswirkungen der Rechte auf die Privatheit der anderen Benutzer:	nein	nein	Ja, dies ist für denjenigen der die Rechte vergibt ersichtlich.
Rollenerstellung und Vergabe:	K.A.	Nur durch autorisierte Personen.	Nur durch autorisierte Personen.
Geltungsbereich der Rechte:	K.A.		
Mehrere Rollen durch einen Benutzer in einem Kurs einnehmbar:	Ja, in einem Kurs.	Ja, in einem Kurs.	Ja, in einem Kurs.
Protokollierung von Zugriffs- und Aktivitätsdaten zur Überwachung des Sicherheitszustandes:	nein	Ja, z.B. Login/Logout, Aufruf von Kursen, Tests	nein
Sicherheitsrelevante Ereig-	ja	ja	ja

nisse einem Verursacher zuordnen:			
Schutz vor unbefugter Einsicht, Löschung und Modifikation:	ja	Ja, Zugriff nur durch autorisierte Personen gem. Berechtigungskonzept von OPAL/OLAT.	ja
Unterstützung der Spezifikation PAPI und IMS LIP:	ja/ja	nein/nein	nein/nein
Lernplattform angemessen gegen externe Angreifer geschützt:	ja	ja	ja
Sichere Login-Passwörter:	nein	Nein, in Opal werden keine Passwörter abgespeichert, da die Authentifizierung der Benutzer direkt an den Hochschul-Nutzerverwaltungssystemen passiert. Identitäten, die in OLAT erzeugt werden, werden automatisch verschlüsselt.	ja
Direkte Einsicht von gespeicherten persönlichen Informationen über die Lernplattform:	ja	ja	ja
Direkte Einsicht von Benutzeraktivitäten und Verbindungsdaten, die vom LMS gespeichert werden:	K.A.	Bei OPAL nur auf Anfrage des Systembetreibers.	nein
Weitere Möglichkeiten:			
Möglichkeit zur direkten Modifikation von personenbezogenen Daten durch den Benutzer:	ja	Bei OPAL: Teilweise. Durch die Identitätsverwaltung an den Hochschulen übermittelte Daten können nicht abgeändert werden.	ja
Benutzer kann festlegen welche Daten über ihn gespeichert werden:	nein	nein	nein
Benutzer kann Zweck konfigurieren, für den seine Daten verwendet werden dürfen:	nein	nein	nein
Benutzer kann entscheiden, welchen Benutzergruppen er seine Daten zugänglich macht:	ja	ja	nein
Benutzer kann einsehen, ob und wer welche persönlichen Daten über ihn abgerufen hat bzw. weiß:	nein	nein	nein
Einwilligungserklärung des Benutzers für die Datenverarbeitung durch LMS zur Verfügung gestellt:	ja	Ja, es wird elektronisch über die Nutzungsbedingungen geregelt.	Ja, sowohl beim Erstlogin, als auch jederzeit unter den persönlichen Benutzereinstellungen ist die Datenschutzerklärung einsehbar.
Widerrufen der Einwilligung:	nein	ja	Nur sofern es sich nicht um

			Angehörige der Universität handelt.
Besondere Sorgfalt bei der Verarbeitung von persönlichen Daten von Kindern:	nein	In OPAL: nein, das es sich um einen geschlossenen Benutzerkreis erwachsener Menschen handelt. Bei OLAT: kann z.B. durch die Organisation des Registrierungsprozesses die Einwilligung der Erziehungsberechtigten erzwungen werden.	nein
Informieren des Benutzers bei Veränderungen der Konditionen der Verarbeitung:	ja	ja	nein
Informieren des Benutzers über die Art der personenbezogenen Daten, die über ihn gesammelt werden sollen:	ja	nein	nein
Informieren des Benutzers über den Verantwortlichen der Datenverarbeitung:	ja	ja	ja
Informieren des Benutzers über den Zweck der Datenverarbeitung:	ja	ja	ja
Informieren des Benutzers über die Sicherheitsvorkehrungen, die zum Schutz der Daten im Einsatz sind:	ja	nein	ja
Informieren des Benutzers, welche anderen Benutzer Zugriff auf seine Daten haben:	nein	nein	ja
Informieren des Benutzers, wenn eine Weitergabe seiner Daten an dritte erfolgt:	ja	Die Weitergabe von Daten aus OPAL an Dritte durch den Systembetreiber wird ausgeschlossen.	ja
Bereitstellung einer Datenschutzerklärung durch das LMS:	ja	ja	ja
Angegebene Zusicherungen durch Benutzer nachprüfbar:	nein	Ja, bei OPAL auf Anfrage beim Systembetreiber.	nein
Pseudonyme Nutzung der Lernplattform:	nein	nein	nein
Anonyme Nutzung der Lernplattform:	nein	Ja, via Gast-Account mit beschränkten Aktivitäten.	nein
Werden mehr sensible Informationen gesammelt als notwendig:	ja	nein	nein
Wird auf die Weiterverarbeitung von Verkehrsdaten verzichtet:	nein	ja	ja
Sensibilisiert die Lernplattform den Benutzer hinsichtlich Datenschutz:	K.A.	Nein OPAL: Bei Zuweisung von Rollen mit erweiterten Rechtenwerden die entsprechenden Nutzer	Ja, die Datenschutzerklärung ist integraler Bestandteil des Erstlogin-Prozesses jedes Benutzers. Ein Überspringen oder ähnliches ist nicht mög-

		geschult und belehrt. Für die Zuweisung einiger Rollen ist eine explizite Datenschutzbelehrung aktenkundig vorzunehmen.	lich.
Wird gewährleistet, dass die Informationen, die über den Benutzer gesammelt werden, wenn benötigt sachlich richtig, vollständig und aktuell sind:	ja	ja OPAL: Es werden Daten, die aus den Hochschulen stammen, verarbeitet.	nein
Kann Zweckbindung technisch durch das LMS überwacht werden?	K.A.	K.A.	K.A
Festlegung des Zweckes der Datenersammlung vor der Erhebung:	ja	ja	ja
Wird gewährleistet, dass nur Personen Zugriff auf personenbezogene Daten erhalten, die sie auch benötigen:	ja	ja	ja
Verknüpfung von Datenbanken und Weiterverarbeitung der Daten:	nein	nein	nein
Ist die Löschung von personenbezogenen und sensiblen Daten durch das LMS vorgesehen:	ja	Nein, aber die Funktion des Löschens von Benutzern und der damit einhergehenden Anonymisierung von Verlaufsdaten wird für OLAT derzeit entwickelt (Version 5.2)	nein
Löschfristen, wenn Erforderlichkeit wegfällt:	nein	K.A.	K.A.
Archivierung von personenbezogenen Daten:	nein	nein	nein
Anonymisieren von personenbezogenen Daten, wenn nicht gelöscht:	nein	K.A.	nein
Handhabung von Kommunikationsdaten, wie Chataufzeichnungen oder Diskussionsbeiträge in Foren:	K.A.	Verlaufsdaten aus Kursen werden mit dem Löschen der Kurse ebenfalls gelöscht.	Dies obliegt den Veranstaltern der jeweiligen Kurse, ob diese zum Beispiel Foren und Chats löschen.
Zusatz:			

	Moodle		
Version	1.5.2 (über 600 Benutzer)		
Unterstützung einer gesicherten Übertragung von sensiblen und persönlichen Daten über das Internet durch das LMS:	Ja, mittels SSL ist eine gesicherte Übertragung immer möglich.		
Konfigurationsmöglichkeiten:	Ja, durch autorisierte Personen.		
Standarteinstellungen:	Keine gesicherte Übertragung.		
Unterstützung einer geschützten Datenhaltung von sensiblen und persönlichen Daten:	K.A.		
Konfiguration:	K.A.		
Standarteinstellung:	K.A.		
Eindeutige Authentifizierung eines Benutzers:	ja		
Rollenmodell:	ja		
Rechte und deren technische Durchsetzung:	Pflichten und Rechte je nach vergebener Rolle.		
Auskunft über Auswirkungen der Rechte auf die Privatheit der anderen Benutzer:	K.A.		
Rollenerstellung und Vergabe:	Administrator allgemein, Lehrer für Kurse.		
Geltungsbereich der Rechte:	K.A.		
Mehrere Rollen durch einen Benutzer in einem Kurs einnehmbar:	K.A.		
Protokollierung von Zugriffs- und Aktivitätsdaten zur Überwachung des Sicherheitszustandes:	Es wird gespeichert welcher Benutzer mit welcher IP-Adresse wann welche Aktionen ausgeführt hat.		
Sicherheitsrelevante Ereignisse einem Verursacher zuordnen:	Ja, durch Protokollierung.		
Schutz vor unbefugter Einsicht, Löschung und Modifikation:	K.A.		
Unterstützung der Spezifikation PAPI und IMS LIP:	nein/nein		
Lernplattform angemessen gegen externe Angreifer geschützt:	nein		
Sichere Login-Passwörter:	Passwörter werden durch den jeweiligen Benutzer festgelegt.		
Direkte Einsicht von gespeicherten persönlichen Informationen über die Lernplattform:	ja		

Direkte Einsicht von Benutzeraktivitäten und Verbindungsdaten, die vom LMS gespeichert werden:	K.A.		
Weitere Möglichkeiten:			
Möglichkeit zur direkten Modifikation von personenbezogenen Daten durch den Benutzer:	ja		
Benutzer kann festlegen welche Daten über ihn gespeichert werden:	K.A.		
Benutzer kann Zweck konfigurieren, für den seine Daten verwendet werden dürfen:	nein		
Benutzer kann entscheiden, welchen Benutzergruppen er seine Daten zugänglich macht:	K.A.		
Benutzer kann einsehen, ob und wer welche persönlichen Daten über ihn abgerufen hat bzw. weiß:	Nein, das kann nur der Administrator.		
Einwilligungserklärung des Benutzers für die Datenverarbeitung durch LMS zur Verfügung gestellt:	nein		
Widerrufen der Einwilligung:	-		
Besondere Sorgfalt bei der Verarbeitung von persönlichen Daten von Kindern:	nein		
Informieren des Benutzers bei Veränderungen der Konditionen der Verarbeitung:	-		
Informieren des Benutzers über die Art der personenbezogenen Daten, die über ihn gesammelt werden sollen:	Nein, aber er kann sie einsehen.		
Informieren des Benutzers über den Verantwortlichen der Datenverarbeitung:	nein		
Informieren des Benutzers über den Zweck der Datenverarbeitung:	nein		
Informieren des Benutzers über die Sicherheitsvorkehrungen, die zum Schutz der Daten im Einsatz sind:	nein		
Informieren des Benutzers, welche anderen Benutzer Zugriff auf seine Daten haben:	nein		
Informieren des Benutzers, wenn eine Weitergabe seiner Daten an dritte erfolgt:	Nein, aber eine Weitergabe ist auch nicht geplant.		
Bereitstellung einer Datenschutzerklärung durch das LMS:	nein		

Angegebene Zusicherungen durch Benutzer nachprüfbar:	nein		
Pseudonyme Nutzung der Lernplattform:	nein		
Anonyme Nutzung der Lernplattform:	Ja, mittels Gastzugang ist eine eingeschränkte, anonyme Verwendung möglich.		
Werden mehr sensible Informationen gesammelt als notwendig:	K.A.		
Wird auf die Weiterverarbeitung von Verkehrsdaten verzichtet:	K.A.		
Sensibilisiert die Lernplattform den Benutzer hinsichtlich Datenschutz:	K.A.		
Wird gewährleistet, dass die Informationen, die über den Benutzer gesammelt werden, wenn benötigt sachlich richtig, vollständig und aktuell sind:	Die Daten werden durch den Benutzer selbst angegeben.		
Kann Zweckbindung technisch durch das LMS überwacht werden?	K.A.		
Festlegung des Zweckes der Datenersammlung vor der Erhebung:	nein		
Wird gewährleistet, dass nur Personen Zugriff auf personenbezogene Daten erhalten, die sie auch benötigen:	Ja, Lehrer und Kursteilnehmer.		
Verknüpfung von Datenbanken und Weiterverarbeitung der Daten:	nein		
Ist die Löschung von personenbezogenen und sensiblen Daten durch das LMS vorgesehen:	Noch keine Planung diesbezüglich.		
Löschfristen, wenn Erforderlichkeit wegfällt:	nein		
Archivierung von personenbezogenen Daten:	ja		
Anonymisieren von personenbezogenen Daten, wenn nicht gelöscht:	nein		
Handhabung von Kommunikationsdaten, wie Chataufzeichnungen oder Diskussionsbeiträge in Foren:	K.A.		
Zusatz:			

K.A. = keine Angabe